CONTENTS

EDITORIAL

FEATURES

CONTENTS...cont'd

EDITORIAL

"It would appear that we have reached the limits of what it is possible to achieve with computer technology, although one should be careful with such statements, as they tend to sound pretty silly in 5 years."

John Von Neumann
(ca. 1949) (1903-1957)
Great Mathematician & one of the
pioneers of modern computing

For many armed forces in the world, including Singapore's, advancements in technology have contributed to a revolution in military affairs. Demonstrating its potential in Desert Storm, and more recently in Operation Iraqi Freedom, technology is the element that has made precision-strike possible and Network-Centric Warfare within reach. There is no doubt that technology is a huge enabler. However, technology alone cannot guarantee victories. In the recent past, we have witnessed military superpowers being defeated by technologically inferior forces, for example the United States in Vietnam and the Soviet Union in Afghanistan. Thus, technology should be seen as a means to an end, but not an end by itself. To be successful in battle, besides technology, armed forces will still need to consider basic combat elements such as firepower, mobility, command & control, logistics, intelligence and protection. Despite its limitations however, technology should not be deprived of its rightful place. Technology has made possible many things that some of us now take for granted and will provide the foundation for many possibilities that today we can

only dream of. To have that cutting edge, we must keep our minds open, be aware of the technologies that are available, and harness them to make the SAF more efficient and effective, relevant in the rapidly changing security environment.

In this issue, we are honoured to feature an article *Harnessing Commercial Technologies to Tackle Intelligence Information Overload* by BG Bernard Tan, Director Joint Intelligence Directorate, and CPT Tan Yueh Phern. Confronted by new challenges of the information age, the authors provide a glimpse into the intelligence information processing chain and survey commercial information-communication technologies that will revolutionise the way intelligence agencies conduct their business. To rapidly harness these exciting tools, they contend that the SAF must fundamentally change its approach towards the technology development cycle and allow a more entrepreneurial playful spirit towards acquiring relevant technologies.

We are also delighted to publish the article *Complexity: Implication for Network Enabled Effects-Based Operations* by Dr Edward Smith, Jr. The article examines the coordinate sets of actions required to shape the behaviour of friend, foe and neutral in peace, crisis and war in Effects-Based Operations (EBO), the complexity of the task, and its implication for Network Enabled EBO. He concludes that the paradox is complexity simplifies, but he deems that the challenge is not all or nothing - sophisticated networking capabilities add to the probability of good human decision-making, but their absence does not make EBO impossible.

In Tech Edge, we are privileged to publish the article *The Seven Technology Challenges for IKC2* by Mr Teo Chin Hock, Dr Yeoh Lean Weng, LTC Chew Lock Pin and Mr Teo Tiat Leng. In this article, the authors show how seven key technological areas can be leveraged to realise a quantum leap in operational capabilities. They conclude that these seven technological areas would underlie the SAF's RMA in IKC2, but while the technologies offer a foundation for many new possibilities to arise, it is up to the ingenuity of people to harness the asymmetry of such technologies, and break new ground in both concepts and technology.

In this issue, we are pleased to publish the article *Myth or Real: Network-Centric Warfare and Integrated Command and Control for the SAF?* by COL Lim Seng Hock. He discusses the concept and evolution of Network-Centric Warfare and Effects-Based Operations, and the tremendous benefits that can be potentially harnessed. He also highlights the significant challenges faced in embarking on the transformation journey, and elaborates on the significant impediments relating to culture, structures and processes, and products that must be addressed before military forces, like the Singapore Armed Forces (SAF) and its IKC2 framework, can achieve integrated command and control capabilities.

We are also glad to publish three winning essays from CDF Essay Competition 2005. The top essay, *Globalization and Transnational Terrorism: Ironies, Interactions and Implications* by LTA Edward Wee, explores the complex relationship between globalization and terrorism, and argues that globalization has fundamentally changed the nature of terrorism. He deems that globalization is a double-edged sword, and just as it facilitates transnational terrorism, globalization can also be used as a weapon against it.

Another winning essay, *Modern Peacekeeping Operations and its implications on the role of militaries in Asia* by LTC Benedict Ang, examines the 'new world order' since the end of the Cold War and why traditional methods of peacekeeping have been inadequate and failed. He elaborates on the growing demands and complexities of modern peacekeeping operations, the challenges faced and their implications on the role of militaries in Asia.

In *Transforming an Army: Military Leadership and Military Transformation in the British and Indian Armies*, LTA(NS) Toh Boon Ho approaches transformation from an unique angle. Unlike the current Revolution in Military Affairs and transformation that requires a fundamental shift in the way warfare is conducted to achieve a quantum leap in operational capabilities, he examines the contrasting styles of Field Marshals Bernard Montgomery and William Slim, and elaborates on the key factors that transformed the British and Indian Armies from mere novices in the field to masters of their craft during World War Two.

We would like to thank all participants, as well as congratulate all the winners of CDF Essay Competition 2005. We would also like to announce that CDF Essay Competition 2006 is now open. The entry form is enclosed in this issue, and do check our website for more details. We look forward to receiving your entries.

Happy reading!

Editor, *POINTER*

Harnessing Commercial Technologies to Tackle Intelligence Information Overload

by BG Bernard Tan and CPT Tan Yueh Phern

Today, we swim in a sea of information. The distribution of traditional media through satellite and cable, and the proliferation of the Internet through fixed line and wireless broadband, have made information available to any individual at almost every spot in the world. As individuals, we have access to probably more information than we need. We are selective in what we want to know. We tune out the rest.[1]

Intelligence agencies however do not have this luxury. Intelligence agencies thrive on volumes of raw data – desiring to sieve out those critical pieces, those gems that will help them make sense of an ever changing situation. But information is only useful if it is pieced together and processed in a timely manner. The trouble is, for most intelligence agencies, the ability to collect information far outstrips their ability to process it.

This has become the key bottleneck in most intelligence agencies. While incrementally expanding the current capacity to process information has been an immediate route taken by many intelligence agencies in the West[2], this is only a temporary palliative. The bottleneck will simply reappear again at a later stage. To get off this conveyor belt, intelligence agencies must allow technology to revolutionise the way they do business and fundamentally transform the processes so that they can cope with even larger volumes, and still come out ahead.

The US Central Intelligence Agency (CIA) was so convinced that it had to tap on the wider commercial market to do this that it took a revolutionary step of setting up a venture fund company called In-Q-Tel. Since its inception in 1999, In-Q-Tel has invested in start up companies with revolutionary technologies that could one day help the CIA fundamentally change the way it trawls and processes data. To date, it has invested in over 90 companies and delivered more than 120 solutions[3] to the US intelligence agencies.

This essay illustrates the types of exciting commercial technologies that can be brought in to help the intelligence community overcome information overload. For the SAF to take advantage of these, its acquisition approach with regard to these software applications must change.

What is In-Q-Tel? In-Q-Tel is the venture capital arm of the CIA. It invests in start up technologies that will allow the US intelligence community to fundamentally better manage information overload. The CIA is doing this, so that promising technologies that may revolutionise its work will not suffer from the lack of initial seed or early stage funding. In-Q-Tel also allows the CIA a less constrained or secretive way in which it can interact with the commercial world and bring in cutting edge commercial technology. In-Q-Tel's investments include the *Keyhole* that delivered a cost effective capability to stream large volume data over relatively low bandwidth networks. Keyhole has since been acquired by Google and its technology is the main pillar behind Google Earth.
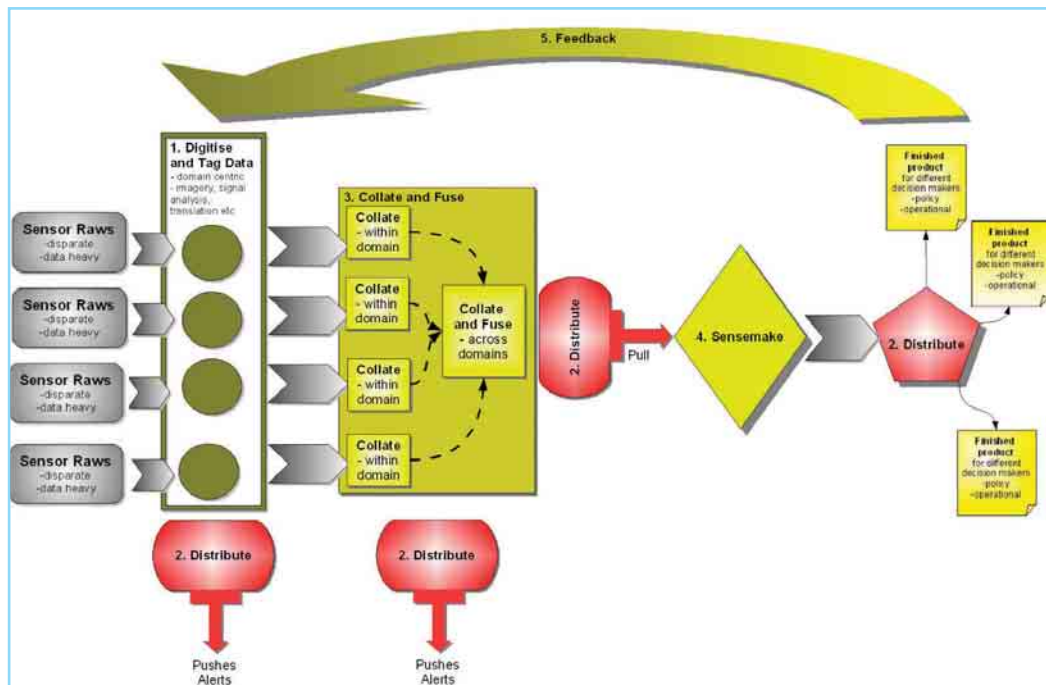

Diagram 1. The Intelligence Information Processing Chain

To understand how technology can help sieve and process information faster, a basic understanding of the intelligence information processing chain is necessary. Diagram 1 offers a simplified version for the reader. In reality, data is never handled in a linear fashion. Raws and products can be returned and recombined into more comprehensive products within the production houses. The modern intelligence production system is probably therefore better described as a ball of strings – consisting of mashes of inter-connected production chains which can return and recombine. Nevertheless, for the purposes of this essay, we will use this simple linear production chain to break down the analysis and production chain into discrete processes and along the way, identify the pertinent enabling technologies that can aid data processing.

Lower End Manual Replacement Tools

Step 1: Digitise and Tag Raw Data. From the left side of the diagram, the first task is to sieve and sort raw data entering the system. Sensors resemble a giant vacuum cleaner that sucks in all available data of varying reliability, accuracy and relevancy. To sieve and sort rapidly, we must leverage on the power of computers. We need to covert raw data into a digital format that can be recognised and manipulated. In its simplest form, information must be tagged not only by time, geography and context, but in accordance to its source reliability, accuracy and its relevance to different areas of interest. This is similar to a librarian's job of indexing books and placing it in the right shelves so that it can be retrieved by users. Of course, given that intelligence data comes from many domains, this librarian not only needs to deal with books, but also free form reports, structured reports, voice tapes, videos, graphics and other types of media.[4] Today's tagging solutions, like XML meta-tagging[5], are largely still manual. They also tend not to be too useful if it is in free form. The United States Department of Defence tried to mandate that all authors create an accompanying summary tag for all their documents. However, over time, these summaries became overly pithy and lost its use as a discriminator.

The fastest way forward is for tagging to be done automatically by computers. There are many applications that are attempting to do this in the market. Riya.com, a Silicon Valley start-up, for example, is trying to use facial recognition and image processing software to automatically scan through photographs to collect visual clues about faces and clothing, and also collect data encoded in the file, such as the time and date of creation. Interestingly, In-Q-Tel is investing in Arabic speech recognition technologies to help better tag voice data. All these technologies attempt to add an additional layer of *auto-tags* created by the software over those tagged by humans.

Looking ahead, the real challenge is to develop auto-tagging technologies that can understand the relevancy, reliability and accuracy of raws to different issues and themes. There are substantial R&D efforts in the underpinning technical domains

such as information theories, natural language processing, image processing and speech analytics that will further enhance the accuracy and relevancy of auto-tags, led by commercial firms such as IBM, Microsoft and Google. With the large amount of resources put into the problem, given enough time, there will be more technical solutions available.

Step 2: Search for Relevant Information, Push Flash. Tagging will help to better sieve data and identify those that are more relevant for processing. In extracting signals from background noises, we must rely on superior search engines. Commercial search engines that depend on suitably indexed databases are available and can be readily employed. Yet, present generation search engines do not really appreciate the meaning of the words one keys in – search results usually rely on statistics, such as frequency that words appears to determine relevancy. Even the most successful search engine, Google, depends on a sort of network analysis[6], as a key criterion in determining the relative relevancy of search results. Such an approach also assumes that intelligence practitioners know what he or she is looking for. In Dave Snowden's domain of "Unknown Unknowns", we may miss weak signals completely. Next generation search engines offer some hope. Software engineers are exploring semantic web applications[7], essentially trying to make the web intelligent and be able to trawl through massive amounts of data to provide accurate answers to user's questions.[8] Some information on next generation search engines are described in the sidebars.

WebFountain. IBM, through her WebFountain supercomputing project, is trying to develop next generation search engines that can mine for meaning and context. Part of the intent is to have the capacity to pick up weak signals. With massive computing power (Its three server clusters runs 768 processors, with the main cluster alone able to store 160 terabytes of compressed data), and using natural language processing based technologies, WebFountain indexes textual documents trawled from the deepest part of the web to analyse casual relationships between each word. IBM claim that the system can identify trends, seek out tiny (and thus tough to pick up) but very valuable nuggets of information and also answer difficult questions like, "What is the marketability of this product?"

There have been some initial demonstrations of the system. In 2002, WebFountain discovered a nugget of precious market intelligence for BP – a small news report of a tiny petrol station in Chicago that created cop-landing areas for police officers. The realisation was that other than petrol prices, crime was also a key factor towards the market's choice of petrol stations.

Given the huge amount of information available, information is primarily organised to be pulled. This is the case on the World Wide Web. However, technologies now allow information to be pushed to the individual.[9] We can, for example, subscribe for alerts to be sent to our cell phones – soccer scores, lottery results, etc. In the intelligence world, we also want critical information to be pushed to subscribers when an event occurs. But given the wide variety of subscribers, what is critical to one party may not be critical to another. Just like in the public world, pushed information needs to be mass customised to each individual subscriber.

The basic level is for the user to define for himself what is the critical information he would like pushed to him. But our interests shift quickly. This is even more true in war. For technology to truly revolutionise the task, the need for users to regularly refresh their interests must be removed. The system must learn what the user is interested in each time the user interacts with the system.[10] Each query is a data point. This is not too different from what occurs on Amazon.com where the system learns more about consumer preferences, the more the consumer interacts with the system. Autonomy, a firm created from research on information systems at Cambridge University, is trying to develop systems with capabilities in pattern matching and interest profiling, to track and automatically analyse user behavior. Essentially, what Autonomy tries to do is to extract pertinent data from the information that users read and create. From this, it develops and also regularly refreshes individual's profile of interest levels in different

topics. Tools like these can potentially revolutionise and become more accurate in the kind of information that is sieved out for the user – allowing him to overcome information overload.

Higher Order Interpretation and Sensemaking Tools

As one moves to the right end of the chain, the processing moves to a higher order. These tools are more complex for they begin to intrude into the cognitive domains.

Step 3: Collate and Fuse. Collation is the process of merging discrete data to make sense of a broader environment. This is done within a single domain – i.e. collating radar plots, or signal intercepts, etc. Whilst manual collation can be tedious and painful, collation is easy for computers. Based on pre-set rules, it is just the simple task of putting tagged data streams together. For better human understanding, one can organise it by various attributes such as time, location or topic. The end-state, however, is still a huge stack of data.

Fusing is the process where collated data are merged across domains – developing a picture from Imagery Intelligence (IMINT), Signal Intelligence (SIGINT) and Human Intelligence (HUMINT). This allows the intelligence system to make 1+1 greater than 2 since each domain both complements and supplements each other. For computers to help in fusion, humans need to set the fusion rules and underlying algorithms[11], and regularly refresh these to reflect the changing dynamics of the battlefield or environment. These rules can span from information on the adversary's orbat, to doctrine, to the assessed psyche

of the political leaders. Beyond manual inputs, the holy grail would of course be a system-of-systems that can update these rules automatically. These are difficult programs to develop, but there is research ongoing in these fields.

Step 4: Make Sense. A completely fused picture of both the physical (land, surface and air) and cognitive environment can be distributed across all users for universal access. However, to make sense of this picture, an analyst must be able to understand the adversary's intent and predict his behaviour. This requires the intelligence system to have a deep understanding of any potential adversaries' behavioural pattern and a profound grasp of geo-political dynamics. There are tools in the market where computers attempt to model such behaviours. Statistical analysis tools, such as Statistical Packages for Social Sciences, have demonstrated limited success in law enforcement and health. However, this is difficult to implement in the area of defence where war is a contest of wills – where deception is the rule of the day. The enemy thrives on doing the unexpected. So this is yet another order of complexity. A system that can do this will need to surmount the very challenging areas of artificial intelligence, machine learning, and theories of the brain model and memory architectures. In the near future, such tasks will probably continue to remain a human activity.

Creating an Intelligent Computer. There are some very exciting work done in this area. One of this is being led by Jeff Hawkins, Chief Technology Officer of Palm Inc and Co-Founder of Numenta. In his book, *On Intelligence*, Jeff Hawkins described a model of how the human brain works – basically that our brain builds sets of beliefs around the cause of various sensed inputs. By creating computers to emulate this model, we can create computers with learning and human cognition capacities. Initial experimental trials showed that the computer could identify various items such as a helicopter and a mug even when viewed from different directions. Hawkins claims that more advanced versions would even be able to take weather data and make weather prediction.

Conclusion

These are exciting times as commercial technologies are developed to help the civilian world manage information overload. Many of these tools can be harnessed by the military

The complexity and challenges of making sense will probably see such tasks remain a human activity.

to overcome information overload within the organisation. To do this, the SAF must move from being a smart developer of unique technology for its own application, to being a **smart buyer and user of commercial information technology**. The way to do this also mandates a fundamental change in the development cycle. Instead of scripting user requirements and SORs, we must allow a far more entrepreneurial playful spirit towards acquiring such technology. We should play around with the latest tools available in the market through rapid experimentation, and see how these tools could be tweaked and harnessed for use by the military. In so doing, we have therefore turned the procurement system on its head. We buy the application having only a hazy idea of how it can be used. We then play around with it, and through this, decide how and where we can use it. We then decide how it must be adapted to make it even more useful. These changes are already taking place given our heavy emphasis on experientation.

The challenge of overcoming information overload will become more important in the years ahead. By 2018, the US Defence Intelligence Agency forecasts that advances in data compression, processing, frequency management, miniaturization and sensors will allow data networks to move voice, data and images at speeds 50 times greater than today.[12] In the 3rd Generation battlefield, it is imperative that the technologies we introduce to manage information will enable the SAF to utilise intelligence and information in a far superior way, to afford the SAF overwhelming advantages in a digitised battlefield. ☺

Endnotes

[1] Of course, there are some who claim that they need to maintain their sanity, choose to tune out completely.

[2] Many have grown by headcount and budget by 20%-30% since 9/11.

[3] In-Q-Tel, about In-Q-Tel. URL: http://www.in-q-tel.com/about/index.htm, accessed on 18 June 2006.

[4] In dealing with videos and voice data, exploitation is presently a laborious manual process. Technologies in Facial Recognition and Speech Recognition will certainly transform the productivity of imagery and communications intelligence processing.

[5] Meta-data can be loosely defined as data describing a particular set of data. Examples includes, time of collection, location and reliability.

[6] The underlying mathematical theorem that governs Google's search engine and rankings is reported in the now legendary paper The Anatomy of a Large-Scale Hypertextual Web Search Engine. Of the various attributes employed to determine relative relevancy of search results, PageRank probably has one of the highest weightage. It studies the links that each webpage has to other webpages and returns an associated number to indicate the relevancy of the webpage to the specified keyword.

[7] Ted Campbell, Semantic Web Gives Clarity to Waves of Data, Defense News Vol 21, No. 25, 19 Jun 2006, (Army Times Publishing Co), p29.

[8] Inxight is one of the leading commercial firms in this area. With her current suite of IT tools, she claim to offer capabilities in analysing textual data (both structure and unstructured) such that key information and relations across multiple data sets can be extracted. They recently secured a $1.7 million USD contract with the US DIA to provide such solutions for the US intelligence.

[9] If one really stare at this for a long time, other issues also pop out: do one push out all raws in flash, or only the ones that are reliable? How does the system judge source reliability and accuracy?

10   Ripeness refers to how much exploitation and processing a piece of raw data has undergone.

11   An example of a fusion rule at the tactical level would be 7 infantry soldiers makes up a section. At the strategic level, a simple example would be, if more than half of the adversaries' forces are destroyed, they are expected to surrender.

12   Defence Intelligence Agency, DIA Workforce of the Future: Creating the Future of the Defence Intelligence Agency, URL: http://www.dia.mil/thisisdia/DIA_Workforce_of_the_Future.pdf, accessed on 1 April 2006, p27.

BG Bernard Tan is currently the Director of Joint Intelligence Directorate. He has held many principal appointments in the Army such as Chief Armour Officer, Assistant Chief of Staff (Plans), and Commander 4 SAB. BG Tan is a President's Scholar and SAF (Overseas) Scholar, and he holds a Bachelor of Social Science (1st Class Honours) in Economics and Political Science from the University of Birmingham, U.K., and a Master of Business Administration from the Massachusetts Institute of Technology, USA.

CPT Tan Yueh Phern is currently an Officer Commanding in Air Photo Unit, Imagery Support Group. An Intelligence Officer by vocation, he was formerly a Platoon Commander in 4 SIR and a Staff Officer in Joint Intelligence Directorate. CPT Tan is a SAF (Overseas) Scholar, and he holds a Bachelor of Science (Civil Engineering) and a Master of Engineering (Biological Engineering) from Cornell University, USA.

Complexity: Implications for Network Enabled Effects-Based Operations

by Dr Edward A. Smith, Jr.

Our world is a complex place, a myriad of ever-changing, interdependent variables whose course we can never entirely predict. The strength – and the challenge – of an effects-based approach to operations is that it squarely addresses this complexity by concentrating on the single most complex aspect of this world: man. Indeed, the entire effects-based approach can be characterized by four things: a focus on the human dimension of competition and conflict; the consideration of a full spectrum of actions whether in peace, crisis, or hostilities; a multi-faceted "whole of nation" concept of power; and the recognition of the complex interconnected nature of the actors and actions involved. The human dimension arises both from the fact that, no matter what form effects-based operations may take, they are ultimately about shaping human perceptions and behavior, and from the fact that

the planning and execution of such operations depend heavily on human beings to make the complex estimates and decisions involved. This human dimension also insists that we consider not just target destruction but an entire spectrum of actions and their impacts across the entire peace-crisis-hostilities continuum. The human dimension also means that the focus is on what observers perceive rather than on what is done and, because any action is therefore but one part of an observed whole, all operations are necessarily whole of nation or whole of coalition in nature. Finally, as all of this implies, any effects-based approach must proceed from recognition that all actions and all the reactions they provoke are inextricably tied together in a system of ever-changing and continually adapting human systems whose complexity fundamentally shapes both the nature of the problem and the task of assessing, planning, and executing any operation military or otherwise.

The central tenet of effects-based operations is that we can somehow purposefully shape the interactions of the actors in this system of systems and the direction of this complex security environment. The definition of effects-based operations as "coordinated sets of actions directed at shaping the behavior of friend, foe and neutral in peace, crisis, and war" underlines the complexity of the task.[1] It does not speak simply of "an action" creating "an effect" in a straightforward, if-this-then-that, cause and effect relationship, but of "coordinated *sets of actions*," that is, the use of multiple interdependent actions. And, it does not look to a single sharply defined effect as the outcome but rather to the actions "shaping" a "behavior" end-state. This is to say it sees both a process and an end-state that are neither precise nor solely the product of the actions we ourselves take. Even more, it does not limit this behavioral outcome to a foe's reactions, but sees "actions" creating diverse effects on many actors at many levels of many different arenas and a requirement for a single set of actions to be able to create opposite effects on foes, friends, neutrals, and the domestic public. In brief, effects-based operations are inherently complex.

"*Shock and Awe*" – *Bombing of Baghdad during Operation Iraqi Freedom*

Complexity

The complexity that shapes the non-linear[2] nature both of the security environment and of effects-based operations can be defined in terms of a continually changing array of interdependent variables in which the chain of causes and effects between an action and an outcome will seldom if ever be the same, in which outputs are not proportionate to inputs, in which the whole is not necessarily equal to the sum of the parts, and in which there will be a nearly infinite number of potential outcomes for any action.[3] How then are we to carry out effects-based

operations much less purposefully to shape the behavior of other actors or the security environment?

Living systems theory offers a way of approaching the problem. It sees the world in biological and sociological terms as an interlocking multi-level system of complex adaptive systems from which no individual system can be extracted without changing both its character and that of the system as a whole.[4] In this system of systems, no interaction can be entirely isolated. Each is part of the continuing succession of interactions by which systems evolve in which each interaction will affect all future interactions in some way. However, the systems in this biological-sociological model do have a recognizable order. In figure 1, we see increasing levels of complexity from the cell through groups, organizations, communities and societies to the international system. All are products of a process of biological and sociological evolution that has weeded out and continues to weed out those systems that simply do not work or that cannot compete. This is important because it tells us that the interactions and outcomes of a system of complex adaptive systems like our world are not infinitely varied and, even more, that we may be able to identify a collection of enduring "essential processes" that explain why these systems survived.[5]
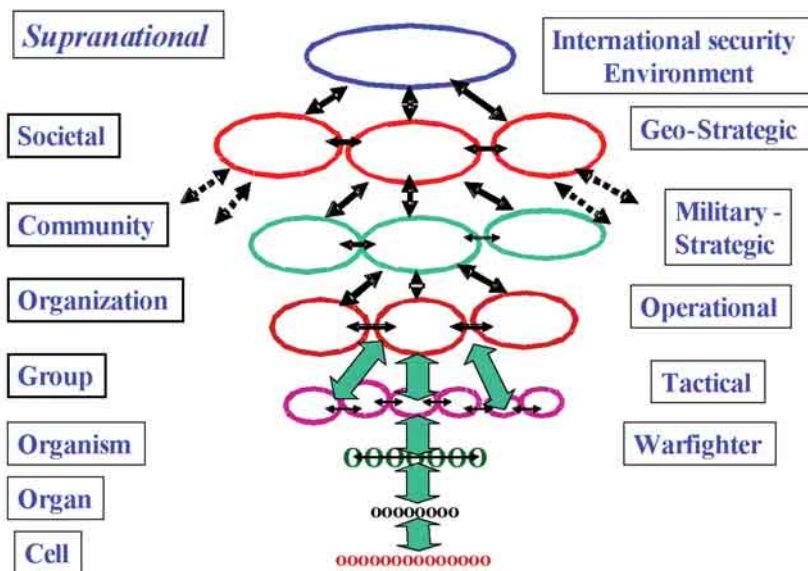

Figure 1. Living Systems Theory – interlocking multi-level system of complex adaptive systems

In effects-based operations, our main concern is with the top five levels of this system of systems from the organism, i.e. man, through his organizations and institutions to the international security environment within which operations must be conducted. In these five systems, (figure 2) we can recognize familiar military organizations from the warfighter, to the tactical unit, to the operational command, to a Ministry of Defense or General Staff, to a national leadership, and to the international arena. Furthermore, because the model is generic to all such systems, we can also make a similar breakdown for other government departments and other states, and for non-state actors, from international and non-governmental organizations to terrorist networks.

The diagram tells us something more as well. It indicates that the interactions that concern us will take place not just at one level, e.g. that of the state, but will occur simultaneously on many different levels. It also suggests – as our real world bears out – that each of these interactions will tend to proceed at a pace dictated by its own local circumstances. Moreover, these multi-level interactions will not just be with a designated foe. At the level of the operational commander (figure 3), for example, we might expect to see interactions with representatives of different government departments and agencies, with allies and neutrals, with non-governmental organizations (NGOs) and international organizations such as NATO or the United Nations as with their agencies, and with the media. Each of these other actors would occupy a position in its own different complexity hierarchy and reporting chain, yet each would also face local challenges and time lines more closely resembling those of their local peers than those of their respective reporting chains. Complexity theory tells us that we should expect these actors to display an emergent, self-organizing behavior, that is, the local actors will tend to build a network of personal relationships to "get the job done" wherever their formal organization permits.
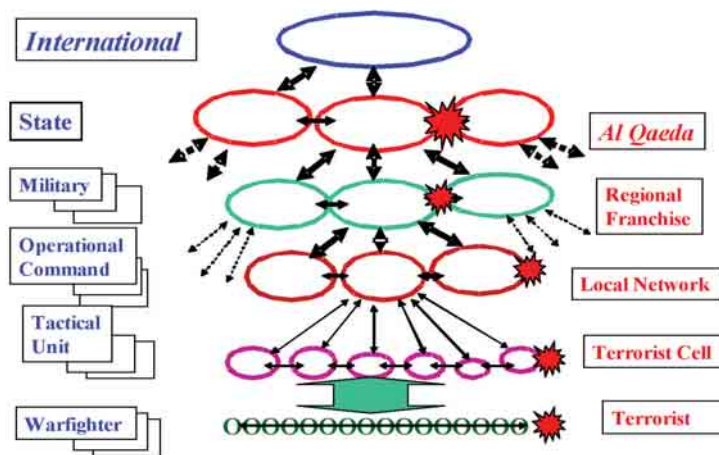
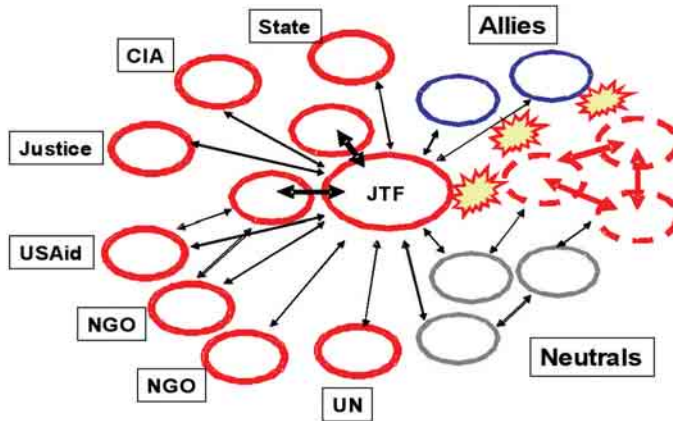

Figure 2. Multi-level Interaction

Figure 3. Cross-section: Organizational/Operational Level

Each of these interactions can be described in terms of an "action-reaction" cycle in which a person or organization reacts and adapts to a stimulus (figure 4). This stimulus will likely be a physical action of some sort – anything from enemy fire, to a diplomatic note, to the initiation of a software program. The stimulus enters the cognitive process through the eyes and ears of an observer who attempts to make sense of it, applies this understanding to judging his options for response, and chooses a course of action or inaction that then becomes both the end-state of the cycle and the stimulus for a new cycle, this time with the other side reacting – a process that will continue in an on-going spiral of cycles each of which builds on what has gone before and shapes those that will follow.

However, this cycle describes how humans and organizations *in general* decide and act, a "rational" man logical framework that, given the nearly infinite number of interdependent variables involved in any real world interaction, will never fully apply to the situation at hand. For effects-based operations, we need to know not only how actors are the same but also how individuals and groups might *differ* either from one another or from a general model. To do this, we must add a social domain[6] that encompasses all of the idiosyncratic variables influencing how particular observers might react *differently* in perceiving, understanding, making sense of a situation and viewing their options. This distinction is critical in deciding which actions, seen how, might shape behavior in a specific way.

Taking a hint from the living systems model, we can examine these interactions to find out why and how the cycle functions, that is, to identify the "essential processes" involved. In fact, we can identify five effects-based "essential processes" that parallel and embody the living system essential processes common (figure 5). Logically, each actor at whatever level in our system of complex systems

Figure 4. The Action-Reaction Cycle

would need (1) to create some level of awareness of what was going on; (2) to make enough sense of this picture to act or react; (3) to decide on a course of action to deal with the challenges presented; (4) to carry out those actions; and (5) in doing all of this, each would be subject to an idiosyncratic array of social influences that would shape both their sense-making and decisions. That is:

- Awareness creation
- Sensemaking
- Decision-making
- Execution
- Social influences.

Figure 5. Essential Processes

Network Enabled Effects–Based Operations

If we accept that effects-based operations by whatever name we may call them are not new and that good commanders have attempted to conduct them since the time of Sun Tzu, then we should be able to trace these processes through real world operations to find out how good commanders have dealt with the complexities involved. One picture that emerges from looking at such commanders is that they use a "man in the loop" to make complex decisions, to assess ambiguous information, and to fill in the blanks where information was wanting.[7] If we look more closely at the roles these human decision-makers played, we can further break the five processes into series of generic problems to be faced, questions to be answered, and issues to be resolved by each decision-maker in undertaking the process and, by further extension, the requirements for information and knowledge that each had. For example, we might break the awareness creation essential process into three main tasks, tasking, collection and analysis and then break these in turn down into more specific problems, questions, and issues (figure 6). Then, each of these might be broken down into a list of subordinate tasks and so on until we could separate those problems that are irretrievably complex (in white) and, therefore, require human intervention and those that may be subject to some form of analysis (shaded) and, therefore, might be areas in which the human might be supported with better information and tools.

Figure 6. Awareness Creation Essential Process

Notice that what we are trying to do here is not to "solve" the complex problems involved. Complexity tells us that, given the myriad of ever-changing interdependent variables involved, we cannot really solve. Rather, we are applying a principle that the author has termed "complexity by contamination", the realization that just because the problem as a wh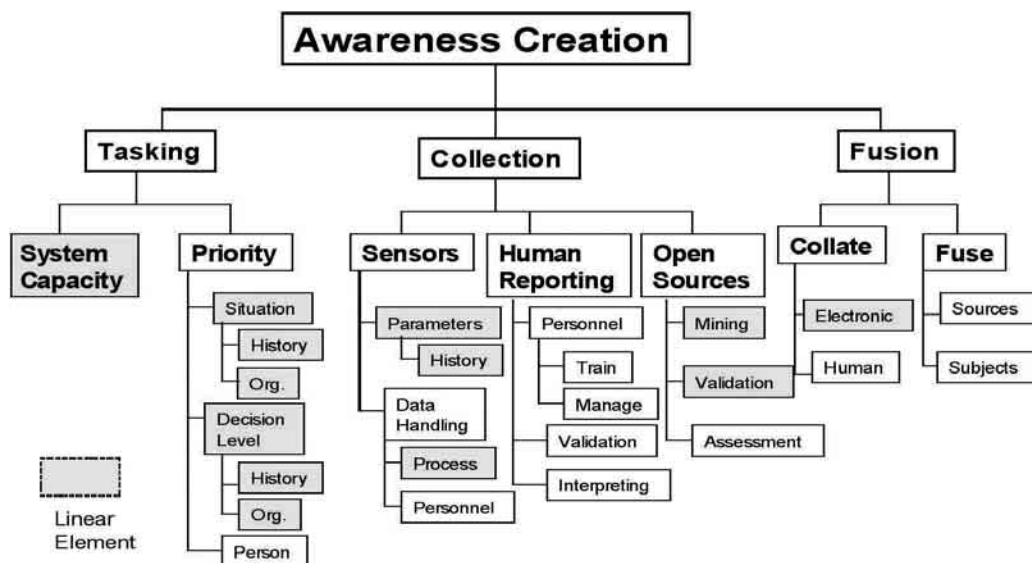ole is complex it does not mean that all its parts are complex. Thus, the more we know of those elements of the problem that are subject to linear analysis, the better able the "human in the loop" will be to bound a set of most likely answers.

This idea is at the root of a network enabled effects-based operations. Success in what might be called "classic" effects-based operations largely depended on the genius quotient – the ability of the human decision-makers involved to do all of the complex work in their heads. In network enabled effects-based operations, the decision-maker need no longer be left to his own devices. The better and more meaningful the knowledge and information support we can provide to the decision-makers, the better able they will be to bound the problems they face and deal with the ambiguities and complexities inherent to effects-based operations – and the higher their probability of a correct decision.

What we have done here is to use the essential processes to define the effects-based problem around the man in the loop and the specific tasks he must perform. In so doing, we have taken a large complex problem that we cannot really solve, have accepted the necessity of human intervention, and have focused the networking efforts

on supporting such intervention. In essence, we have made the complex effects-based problem divisible and have made it subject to a step by step approach whose metric is the probability of a correct decision.

Scalability and Timeliness

There is something that is missing from this picture. Given a multi-level system of complex adaptive such as we have outlined, effects-based operations clearly need to be both dynamic and scalable down to the tactical level. Yet, there seems to be a stark contradiction between the apparently rather ponderous and time-consuming process of dissecting action-reaction cycles on the one hand and the requirement for dealing with an adaptive foe in an ever-changing situation on the other. It would, therefore, be easy to conclude at this point that effects-based operations can only be planned and assessed at the operational level of war or higher, that is, in situations where timelines are longer and where the personnel and assets exist to undertake such a detailed process.

Yet, such a conclusion would fly in the face of what we are already routinely doing in the field. Over the past 60 years, for example, there have been around 400 crisis response operations by U.S. military forces.[8] Few of these involved actual combat; all were in one fashion or another about the human dimension of competition and conflict; all involved an integrated application of national power; and all were by those measures effects-based. But strikingly, few involved large staffs and elaborate planning processes to do all of this.[9] Even more telling are the reports of

current tactical operations. One good example is the response of a young U.S. Army Captain to a journalist's query as to why he and his unit had just engaged in a six hour firefight with insurgents over a burnt-out Humvee: "We weren't going to let them dance on it for the news…even with all the guys they lost that day, that still would have given them the victory."[10] The Captain was aware of the multiple dimensions of the firefight, had a sense both of the diverse observers of the interaction and of the role of an effects-based metric for "victory" in his decision-making and execution. And, he was able to use his understanding of command intent to execute action-reaction cycles at the minute by minute speed of battle.

How did these operational and tactical level commanders do it? Part of the answer (figure 7) lies in looking at an effects-based interaction not as an intricate staff planning process but in its essentials as nothing more than an elaborate Observe, Orient, Decide and Act (OODA) loop in which the awareness creation is the *observe* phase, the sensemaking the *orient* phase, the decision-making the *decide* phase, and the execution the *act* – all of which can be jammed into a real world give and take cycle that may last but 90 seconds or less.

The OODA loop as originally presented by Colonel John Boyd offers three advantages: it is rapid; it is scalable; and it is cyclical and, thus, continuous.[11] Even more, the OODA loop also presumes a continued interaction between two or more actors with changes in the actions of one driving the changes in the action of the other, much as it was carried out by pilots in the aerial maneuvers that Boyd studied. The OODA loop recognizes an underlying reality both of military
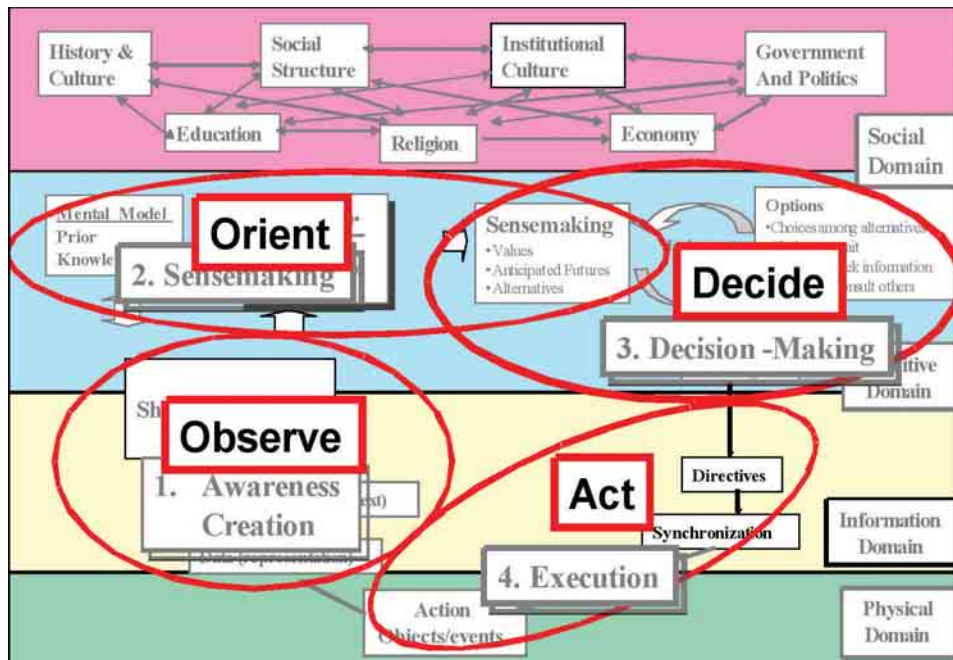

Figure 7. OODA Cycle

operations in general and of effects-based operations in particular: that timing is everything. There simply will not always be time for an involved planning process. Rather, the OODA loop has to be internalized by training and experience to the point that it became almost intuitive. The same appears possible with the man in the loop of effects-based operations.

US Planners in Operation Iraqi Freedom

Implications

The role of the man in the loop in real world operations is marked by a four-fold trade:

- The greater the uncertainties, ambiguities, and unknowables in a problem, the greater is the requirement for human intervention;
- The greater the complexity of the problem, the greater is the human role;
- The less the time available for decision-making, the greater is the role of the human in making that decision; and
- The less the support available, the more the human is called upon to do.

The first three of these trade-offs will come as no mystery to anyone who has been in combat. All three have been reflected in classic, human centered approaches to effects-based operations and in efforts to choose and form the right decision-makers to provide the needed "genius quotient" as well as in efforts to provide the organizational latitude and agility necessary for them to function. But, it is in the latter trade off between support and the requirement for human intervention that the potential for a new human centered but network enabled version of effects-based operations becomes evident.

In the first flush of network-centric operations, efforts to exploit Information Age tools tended to focus on taking man out of the loop so as to decrease human error and increase speed of command. Networked communications also seemed to offer a way to centralize decision-making at higher levels of command and to linearize the planning of complex operations. However, "first generation" network centric operations quickly ran afoul of real world complexities. Taking man out of the loop to create "sensor to shooter" architectures, for example, only applied to the relatively narrow part of the operational spectrum where pesky complex variables could be assumed away. Centralizing direction at higher levels although a necessary element in achieving unity of effect, also reduces the ability of "edge" commanders to adapt and survive in fast paced local interactions. And the limitations of the "man out of the loop" approach are even more evident in effects-based operations with their human dimension, their vast operational spectrum, their whole of nation character, and their inherent complexity encompassing very large numbers of continually changing interdependent variables.

In a sense, effects-based operations drive us to a different version of network centric operations. The network exists to facilitate the needed decision-makers' intervention by bounding the problems with which the human must deal. Networking in this context encompasses the tools and linkages needed to do everything from applying data mining to sorting human reporting in open and closed source material, to intelligent agents and gaming techniques to assess the consequences of a prospective action, to cognitive, social, and cultural anthropological models, to the role of subject matter experts either in direct support or in putting a "reality check" on modeling and gaming efforts. Even more, the demands of a system of complex adaptive systems mean that we can no longer think solely in terms of static communications architectures, but must think of a "second generation" of *networking* that continually changes – sometimes very rapidly – as the environment and situation mutate and that resembles more a continually evolving mesh of relationships that is relatively unbounded in scope.

These demands and the human intervention trade-offs suggest a four fold metric for second generation network centric operations:

• The more networking can reduce the uncertainties and ambiguities, the less human intervention will be required;
• The more networking can bound the complexities of the problem, the less the human in the loop will need to do;
• The more time networking can provide for decision-making, the less often the human in the loop will be the final resort; and

• The more the networking can provide, the greater will be the probability of the human making the correct decision.

The true metric for both second generation network centric operations and for network enabled effects-based operations is thus the quality of the human decision making that emerges.

Conclusion

The central issue in effects-based operations is not whether or not to do them. We already can do them and, in an increasingly complex world of asymmetric foes in which traditional attrition-based models of state-on-state conflict do not work very well, we have little choice but to pursue an effects-based approach. The real question confronting us is how to do them *better.*

The description of the systems of complex adaptive living systems that constitute our world seems daunting and doubly so in the context of conducting human-centered, cross-spectrum, whole of coalition operations. However, there is a paradox here: complexity simplifies. If we accept the innate complexity of what we are trying to accomplish, then we accept too that there cannot be perfect awareness, that we will never have all the answers and that we will never entirely understand our adversaries – or for that matter the friends and neutrals with whom we work. We accept too that we cannot "solve" the problem and can never plot all possible consequences of our actions. And, we accept the need for the human being – that product of

biological evolution and genitor of sociological evolution and a complex adaptive system in his own right – as key. Complexity in short sets a relative standard for decision-making: that it is sufficient to do all of these things better than our would-be opponents.

Clearly, there are many Information Age capabilities that can help us do better in dealing with this complex world, but the key facet of network enabling is that an Information Age network must above all else link people and that the problem is as much about agile organization and social networking as it is about communications architectures. This is not to dismiss the value of better communications but rather to define what is needed in human terms and in terms of a continually changing challenge. It is to think in terms of an evolving, adapting social and communications networking that changes with the problem.

Finally, notice that, in the networking metrics as in the earlier trade-offs, there is a message. The absence of a sophisticated networking capability does not make effects-based operations impossible; it just means that the resulting operations will more closely resemble the classic, human-based approach. The challenge is not "all or nothing". If we define it in terms of adding to the probability of good decisions by the human in the loop, we can build in pragmatic finite steps each of which promises in some way to better human decision-making.

Endnotes

1 Edward A. Smith, Jr., *Effects-Based Operations* (CCRP: Washington, D.C. 2002), p108.

2 Perrow defines "complex" or non-linear in terms of "interactions in an unexpected sequence" as opposed to "linear" which he defines as "interactions in an expected sequence"
Charles Perrow, *Normal Accidents, Living with High-Risk Technologies* (Basic: New York, 1984), p78.

3 In defining complexity as "conceptual equipment for policy-makers," James Rosenau points to four basic ideas embodied in complexity theory: 1. self-organization and emergence or the ability of the parts of a complex system to change and deal with change while preserving an internal dynamic; 2. adaptation and co-evolution or the ability to adapt to or co-evolve with the surrounding environment; 3. the power of small events to throw a system into disequilibrium and thus set off a reaction very disproportionate to the stimulus, e.g. the butterfly effect where the flapping of a butterfly's wings in China might provoke a hurricane in the Atlantic; and 4. sensitivity to initial conditions or the ability of only slight changes in the initial conditions can result in very large downstream changes.
James Rosenau, "Many Damn Things Simultaneously" in *Complexity, Global Politics and National Security.* David S. Alberts and Thomas J. Czerwinski eds. (National Defense University: Washington, D.C., 1997), pp84-87.

4 James Grier Miller, *Living Systems* (University of Colorado: Denver, 1995) p854.

5 Miller identifies 23 such essential processes to be found in the complex adaptive systems at each level of the model.
Miller, pxvii.

6 David S. Alberts and Richard Hayes, *Power to the Edge* (CCRP: Washington, D.C., 2003), p113.

7 To this end, the author used firsthand observations of a series of crisis operations by the Battle Force of the US Sixth Fleet in 1986 and 1987 first under RADM David Jeremiah, later Commander in Chief Pacific and Vice Chairman of the Joint Chiefs of Staff and then under RADM Mike Boorda, later NATO's Commander in Chief South during Bosnia operations and then Chief of Naval Operations.
Smith, *Effects-Based Operations*, chaps 10 and 11.

8   These figures are derived using the methodology developed by Barry Blechman and Stephen Kaplan in *Force without War* and subsequently extended by various authors. Blechman and Kaplan, *Force without War* (Brookings: Washington, D.C., 1978). Zelikow, Philip D. "Force with War, 1975-1982", *Journal of Strategic Studies* (March 1984). Siegel, Adam, *The Use of Naval Forces in the Post War Era* (Alexandria: Virginia, CNA, 1991).

9   The previously cited Sixth Fleet Battle Force operations in 1986 and 1987, for example, were executed with a 20 man staff.

10 Scott Wilson, *Washington Post* (June 26, 2004).

11 Colonel John A Boyd USAF, "A Discourse on Winning and Losing" Air University Lecture (1987).

Dr Edward A. Smith, Jr. is currently the Executive Strategist for Effects-Based Operations at The Boeing Company. He is a retired U.S. Navy Captain, and during his 30 years of service, he had flown some 200 combat missions in Vietnam, and was on the staff of Battle Force U.S. Sixth Fleet during the Achille Lauro and Libyan contingencies in 1986 and 1987. He had also served in the Defence Intelligence Agency, in the Office of Naval Intelligence, and on the personal staff of the Chief of Naval Operations. Dr Smith holds a PhD in International Relations from The American University, and he has written widely on Network-Centric Warfare and Effects-Based Operations. His latest book is Complexity, Networking, and Effects-Based Operations published by the U.S. Department of Defense Cooperative C4ISR Research Project.

Myth or Real : Network-Centric Warfare and Integrated Command and Control for the SAF?

by COL Lim Seng Hock

"*By making possible a faster, clearer reading of the situation and a more effective distribution of resources, a superior command system may serve as a force multiplier and compensate for weaknesses in other fields…*"[1]

·Martin van Creveld, 1985

Introduction

New ways of thinking about command and control (C2) are at the heart of Information Age Warfare.[2] The increasing complexity of military weapons systems, military organizations and war-fighting itself, have created an ever-increasing demand for and reliance on information technology systems.[3] The emergence of what is termed as the Revolution in Military Affairs (RMA) is generally accepted by many military services (i.e. the advent of knowledge warfare or information age warfare).

Advancements in information technology are enabling modern armed forces to undergo a fundamental shift from a platform-centric orientation to a network-centric one. Recently, the concept of Network-Centric Warfare (NCW) has been widely discussed. Network-centric operations are military operations that are enabled by the networking of the force.[4] As such, perspectives about the process of command and control can change fundamentally. A robustly networked force will be integrated vertically by the network, through all command echelons – strategic to tactical and down to the lowest tactical level.[5] While it is usual to focus on the technology portion of the information age influencing the evolution of command, the effect should be viewed as more than just a more effective C2 system.

This essay highlights the significant challenges faced in embarking on this form of transformation journey. The thesis is that it will be some time before military forces undergoing transformation, like the Singapore Armed Forces (SAF), can achieve integrated command and control capability because significant impediments relating to the **culture, structures and processes, and products** must be addressed.

The RMA Debate

Many analysts of the RMA have argued that technological breakthroughs will have a major effect on how operations will be conducted in future. The Gulf War is often cited as an example of how these new technological advances can be employed on the battlefield, based on the success of the high tech weaponry and the command and control systems of the U.S. forces.[6] Some also argued that the rapid conduct of *Operation Allied Force*[7] and the wide-spread use of precision-guided munitions provides further evidence that we are on the verge of a change in how war will be conducted in future.[8]

Although generally accepted, the RMA debate continues because there are several different views of an RMA. Revolutions imply periods of rapid and fundamental changes and are hard to predict because of the expected disruptive effects. There can be little doubt that further scientific revolutions will occur and any defence planning that looks more than 15 to 20 years ahead must be flexible enough to take account of the potential offered by the radically new technologies that may emerge.[9]

For the SAF, new challenges are constantly emerging (e.g. rise of transnational terrorist threats such as the Al Qaeda network). The SAF must be prepared to meet future challenges while meeting the demands of the present. As such, there is a need to have greater flexibility and robustness in the developmental approaches. In its recently published monograph, the need to begin the transformation journey and to meet the complex challenges of technological discontinuities, asymmetry and globalisation were emphasised.[10] The *capacity to change* is as much about looking at fundamentally different strategic "options" as changing the *mindsets* of people to "dare" to look at radical changes and to experiment. The **military culture** is an important consideration if revolutionary operational concepts were to be tested successfully.

NCW and Effects–Based Operations Development

It would be tempting to think that the exploitation of information age technologies in the military environment is essentially a communications, information system or staff process issue. Also, that this will result in a substantive outcome, which will be a more effective command and control system – and that it can be left primarily to those responsible for developing our command and control systems.[11] However, if a more effective C2 system is intended to fight in a very different way, it must be understood and applied by commanders and warfighters, not technical staff.

Over time, information age technology can be exploited by emphasizing an integrated battlespace by exploiting networked capabilities. The shift will be towards a network-centric environment with integration throughout a theatre of operations and between theatres of operations. The emphasis will be on exploiting networked capabilities to apply integrated joint effects to precise effect. "There will be greater emphasis on connectivity between sensors, weapon platforms and C2 nodes and less emphasis on numbers of weapon platforms."[12] These are essence of what is commonly termed Network-Centric Warfare (NCW).

Source: Pioneer

Satellites and Unmanned Aerial Vehicles (UAVs) relay real-time, strategic information of the battle space to the command centre. With enhanced situation awareness, coordination on the ground is improved, as commanders are able to make more informed decisions.

The Command Post is the nerve centre of the battlefield as information from various platforms are collated, processed and relayed to troops on the ground, in the air or at sea.

Autonomous Unmanned Ground Systems (AUGS), soldiers decked out with the Advance Combat Man System (ACMS), and state-of-the-art weapons such as the 40mm Air Bursting Munition System (ABMS) and guided missiles, form a lethal fighting force. Networked with fellow comrades, these small companies of soldiers will be able to see ahead and launch precision strikes.

A glimpse into what is to come

In a way, NCW provides the theory of warfare in the Information Age. It is, as the NCW Report to the U.S. Congress stated, "no less than the embodiment of an Information Age transformation of the DoD".[13] It was stated that the network-centric warfare and all of its associated revolutions in military affairs "grow out of and draw their power from the fundamental changes in American society".[14] Basically, the argument was that the underlying economics (IT is central to competition based on return on investment) and the underlying technologies (e.g. explosive growth of Internet and use of network-centric computing) had changed. With the changes happening in the way business was conducted,[15] the military must also adapt.

NCW is characterized by information sharing, shared situational awareness and the knowledge of commander's intent. A warfighting force that can conduct network-centric operations can be described as having the following attributes and capabilities:[16]

- Physical Domain: all elements of the force are robustly networked achieving secure and seamless connectivity.

- Information Domain: The force has the capability to collect, share, access and protect information. The force can collaborate in the information domain.

- Cognitive Domain: The force has the capability to develop and share high quality situational awareness and have a shared knowledge of the commanders' intent.

One of the major insights that have emerged as a result of ongoing NCW initiatives is that the combat power associated with network-centric operations is non-intuitive.[17] Hence, the likelihood is that warfighters will develop new tactics, techniques and procedures only after they have the opportunity to operate and train with an information advantage and develop trust in the advantage of operating in a networked environment.

In spite of a ponderous acquisition process, technology insertion is ahead of and disconnected from joint and service doctrine and organizational development.[18] This is perhaps one of the reasons why the impediments to progress have also been a subject of debate in the literature. In a recent article on learning lessons about NCW from Operation Iraqi Freedom, it was mentioned that a retired U.S. Marine Corps General had said that many personnel still "have no clue what it is" and that "there's a significant communications problem at the tactical units who were out of contact except for satellites".[19] According to retired Navy Vice Admiral Arthur Cebrowski, not enough technology that drives NCW is finding its way into the hands of the warfighters and that a *change of culture* is also needed to adopt the technology.[20]

The issue of **culture** is an important consideration and will be discussed later as a key factor to consider if the SAF were to succeed in its transformation journey. It has been argued that the Western armies have progressed significantly over the years because of "…a long-standing Western

cultural stance towards rationalism, free inquiry and the dissemination of knowledge…".[21] An overall cultural landscape can therefore afford inherent military advantages in terms of the way the thinking and innovative ideas can develop.

For NCW to be useful, it must be applied to military operations. This is important especially to the operational-level commanders who need to translate the concepts to application in the theatre of operations. Military operations, in the new security environment, will span across the spectrum of operations from peace, to crisis and to war. The common term that is increasingly being use to describe the process to shape the desired result is "*effects-based operations*" or EBO.

Source: Army Recruitment Centre

Operationally ready in peace, crisis, and war

EBO (military operations directed at shaping the behaviour of foes, friends and neutrals, in peace, crisis and war) constitute the conceptual framework for a two-step process of turning network-centric capability into a national advantage.[22] In a way, EBO is not an entirely new thinking since using military forces to shape the behaviour of opponents and allies have been practised since a long time ago. EBO can transcend the levels of operations in order for strategic, operational and tactical objectives to be attained. David Deptula, an early proponent of the concept of EBO,[23] provided a catalyst for much of the conceptual development and debate. Initially, the proponents were mainly from the U.S. Air Force due to the emphasis on air power to achieve strategic effects.

Adaptation to the Information Age will mean an understanding of what NCW and EBO can bring to military operations while bearing in mind that these are still largely terms used by the U.S. researchers and they do not imply a replacement of the forms of warfare. However, they do present a possible synergistic approach in looking at military transformation. EBO encompasses the mind with focus on the mission and the conditions of military operations, while NCW provides the framework and tools. They deal with the why, what, how and support of military operations,[24] which are crucial to looking at the military transformation journey.

Transformation in the Information Age

While some may argue that the NCW is not optimised for asymmetric warfare[25] and low intensity conflict,

NCW is a key component of what is the latest term used in the conceptualisation of RMA: *transformation*. It was reported that the information networks established for the United Kingdom's Iraq War forces paved the way for the country's force transformation.[26] Some of these efforts were driven by the need to interoperate with vital U.S. C4I systems that were rife with imagery.

Worldwide, many modern military forces have crafted their own individual responses to the challenges and opportunities of the information age. NCW is a common term used by the armed forces of the United States, Denmark, Norway and the Netherlands. Other terms coined include Australia's Network-Enabled Warfare[27], the United Kingdom's Network-Enabled Capability, the Swedish Armed Forces' Network-Based Defence and the Singapore Armed Forces' Integrated Knowledge-based Command and Control.[28]

What does the term transformation mean? Dr David Alberts described transformation as "a process of renewal, an adaptation to environment".[29] Essentially, transformation would mean adapting to significant changes and failure to do so would imply risks as well. Alberts argued that potential adversaries can also take advantage of the low cost of obtaining "Information Age technologies" and inaction is not an option in a transformation strategy.[30] Pushed by the U.S. Secretary of Defence Donald Rumsfeld himself, the need to transform was seen as important due to the changing environment (spectrum of operations) and different threats, while the capabilities are evolving.

However, while there are indeed remarkable improvements in developing warfighting concepts in the U.S. armed forces, the same progression has not happened in creating truly ready joint forces in peacetime and the related rationalization of capabilities in the services.[31] This may be offset by a recent development in the Pentagon where the Joint Staff would have greater control by being able to ensure that efforts by the services are not duplicated.[32] Five functional capabilities boards (areas of force application, force protection, battlespace awareness, focused logistics, command and control) would be created to spearhead the analysis, prioritise needs and advise the higher approval committee.

In Singapore's context, the IT landscape has changed significantly and the quest to achieve a high level of competencies in IT related skills among her population are clearly producing results. Today, the SAF has developed into a military that is technologically focused and professionally respected. However, these have also impeded the inertia to change radically for fear of upsetting the efficient and well-established procedures. As such, the transformation journey must also focus on the **people** aspect and involve the operational commanders and men by enabling them to be part of the capability concepts development. For example, they can help to review and validate some of these concepts during command post and field exercises.

Re-conceptualizing Command and Control

The terms 'command', 'control', and 'C2' are terms that are often used in the military literature. They are supposed to be quite entrenched in the doctrinal and operational "dictionary". However, their usage can be said to be "abused" and it is probably true to say that a number in the military may sometimes be confused by the context of their usage. After some research, Pigeau and McCann remarked that "there was little consensus within either the military or the research communities on the actual definitions for Command, Control and C2".[33]

Historically, the topic of command has been extensively discussed and much written regarding its methodologies and practices. The term command and control (C2) appears to be more recent and could be attributed to the advent of IT and its application to the military.[34] Command as defined by the U.S. military includes "responsibility for effectively using available resources, planning the employment of, organizing, directing, coordinating and controlling military forces for the accomplishment of assigned missions. It also includes the responsibility for health, welfare, morale, and discipline of assigned personnel."[35] As such, control is subsumed as a part of command. This view was also echoed recently about how control is more than a feedback mechanism since **structures and processes** must be put in place to facilitate accomplishment of mission.[36]

It may not be fruitful to force a distinction between command and control. Some of the common distinctions argued include between art (command) and science (control) and one between the commander (command) and staff (control).[37] The U.S. DoD's JSP definition of C2 refers to the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.[38] The U.S. Army has also published the new C2 doctrine (Field Manual FM 6-0) *Command and Control* to take into account the development and use of modern IT and "their powerful ability to influence the conduct of operations".[39]

It is better to refer to C2 in the context of processes to achieve the accomplishment of mission, from formulating courses of action to monitoring the execution and giving orders.

However, a growing number of those who are looking at command and control in the Information Age have concluded that the terms need to be clarified and brought into the 21st century,[40] without being constrained too tightly by historical references.

Pigeau and McCann took a new look and defined the two terms separately and in an interesting way:[41]

- "Command: the creative expression of human will necessary to accomplish the mission."
- "Control: those structures and processes devised by command to enable it and to manage risk."

They place an important emphasis on the human aspect of command that can achieve outcomes through motivation

and having the means and opportunity. They include a model to distinguish command that incorporates three factors: Competency, Authority and Responsibility. Their definition of C2 is the establishment of common intent to achieve coordinated action.[42] Hence C2 structures must have the ability to stay *flexible* to meet evolving needs while continual learning and change should be encouraged and rewarded.

C2, in its historical context, refers to the structures (real and imagined), process, technology, and people that comprise the system.[43] For a commander to have effective C2, the system must enable him to make timely decisions and take appropriate action. The well-known Observe, Orientate, Decide, Act cycle (OODA Loop)[44] allows new thinking in reducing the decision-action cycle. It has an intuitive appeal, resulting in the common phrase used by many commanders: "operating inside the enemy's OODA loop". The OODA loop, when applied in the information age context, may appear too simple. For example, it was highlighted that it cannot model correctly the differing C2 processes, both in terms of function and time scale, which are carried out by HQs at various levels of command.[45] One of the useful models to look at when considering the network-centric portion of looking at C2 processes is provided in Figure 1.
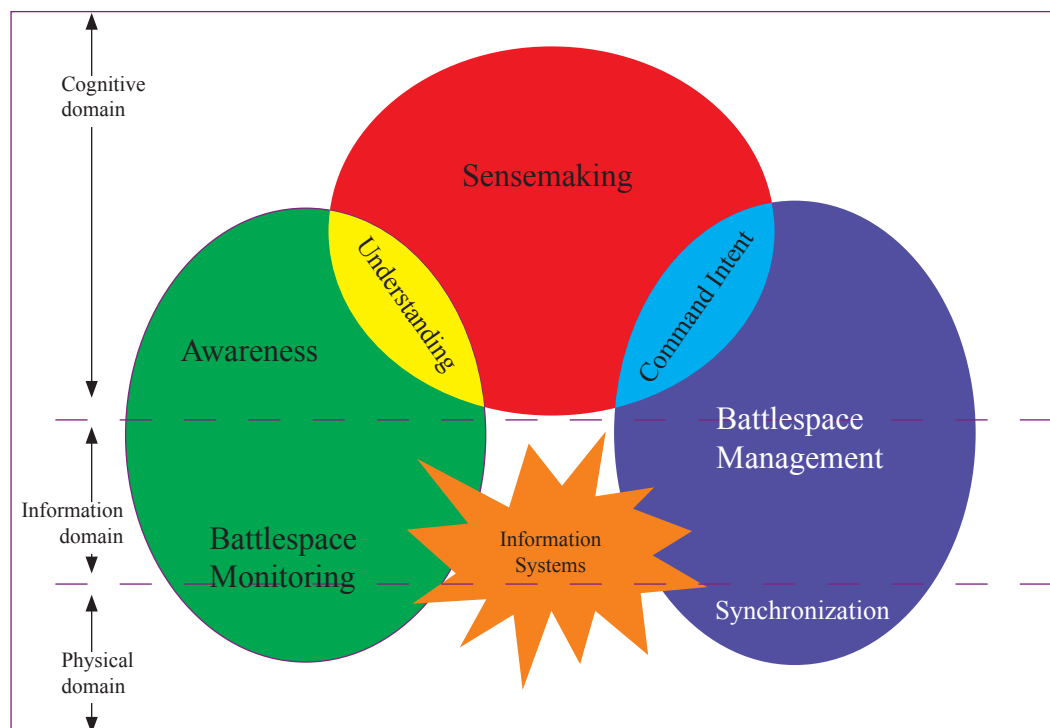

Figure 1. The Information Age C2 Process
[Adapted from David S Alberts, et al, Understanding Information Age Warfare, (CCRP Publication Series, Aug 2001), p146.]

The model consists of three domains that define military activity, which were described earlier as the attributes of NCW. Here, the physical domain consists of the operating environment (entities outside the C4ISR[46] processes and systems) while the cognitive domain refers to the minds of the participants. Within these domains, the interacting elements include battlespace monitoring, awareness, understanding, sensemaking (how situation may develop), command intent, battlespace management (command intent translated into activity) and synchronization.[47]

This model allows one to look at the cognitive domain with the aim of ensuring a better understanding of the situation and the higher command's intent. Battlespace monitoring and management are taken care by the NCW aspects (i.e. sensors' system of systems and seamless information grid). A shared understanding of the operational situation at all levels of command should provide the stage for mission command to flourish and enable an unprecedented tempo of operations and effectiveness of manoeuvre and engagement.[48] This, Alberts proposes, can enable greater integration with a networked C4ISR and the information systems embedded in it.[49] Integration will also imply it will have great impact on the interoperability issue as well.

Integrated Knowledge–based C2 in the SAF

The SAF are in the eyes of many experts, the most competent and experienced in all-arms mobile warfare within ASEAN (Association of Southeast Asian Nations, comprising

10 countries).[50] We are recognized to be able to quickly adopt new technologies into our inventory.[51] The impact of the RMA within the SAF has been most prominent in the area of Integrated Knowledge-based Command and Control (IKC2).

The central idea of IKC2 is the superior collection and organization of knowledge to provide dominant situational awareness to all levels of command to achieve more effective command and control of forces and the precise application of effects.[52] IKC2 aims to maximize combat effectiveness and gives the SAF a quantum jump in capabilities within the constraints of its resources. Command and control is as much about the technology and **processes** that enable it as it is about the commanders and staff who are an integral part of it. *Integrated* refers to the need to fight as an integrated and multi-dimensional force. SAF is still largely organized along Service lines and hence there is a need to plan on the basis of the entire SAF's capabilities and one basic requirement is the integration of the command and control system.[53]

IKC2 enables the SAF to engage in NCW through the use of advanced C4 and IT technology. In a networked environment, a knowledge-based approach that allows sharing of information and knowledge can be embedded in decision support systems, hence allowing commanders and staff to focus on core issues rather than technical analyses. IKC2 works on the OODA loop as a basis and considers the three domains mentioned earlier. Represented in Figure 2, IKC2 aims to "see first, see

more" and therefore result in better understanding and be able to "act decisively". It is envisaged that IKC2 will enable knowledge-based warfighting concepts to be operationalised and to contribute to a more flexible and flatter C2 structure. If the speed of decision-making also increases, then this will enable a higher tempo of operations to be effected.

What does IKC2 imply to the commanders and men? While there is little doubt that IKC2 can change the way we think and the way we fight, much more needs to done to the main components of force transformation: *culture, process and product*. While IKC2 builds on the SAF's comparative advantage of having a relatively large number of techno-savvy people, the development and subsequent changes must be based on a shared purpose approach with the commanders down to the battalion level. After all, integration in C2 implies working towards a common purpose by maximizing resources available.

While the "fruits" of IKC2 will not be borne so quickly due to the existing gap, dialogue with all levels of commanders should always be maintained to highlight development and progress, e.g. testing of concepts and results of C2 related experiments. Intermediate products and knowledge gained (whether successful or not) should be shared widely. To achieve the next big leap in capability, IKC2 *cannot be the dream of just a few and remain distant and vague to the rest.* Transformation is indeed about moving forward and what it means to the soldiers should be a continuous effort so that the journey is made as a cohesive force.
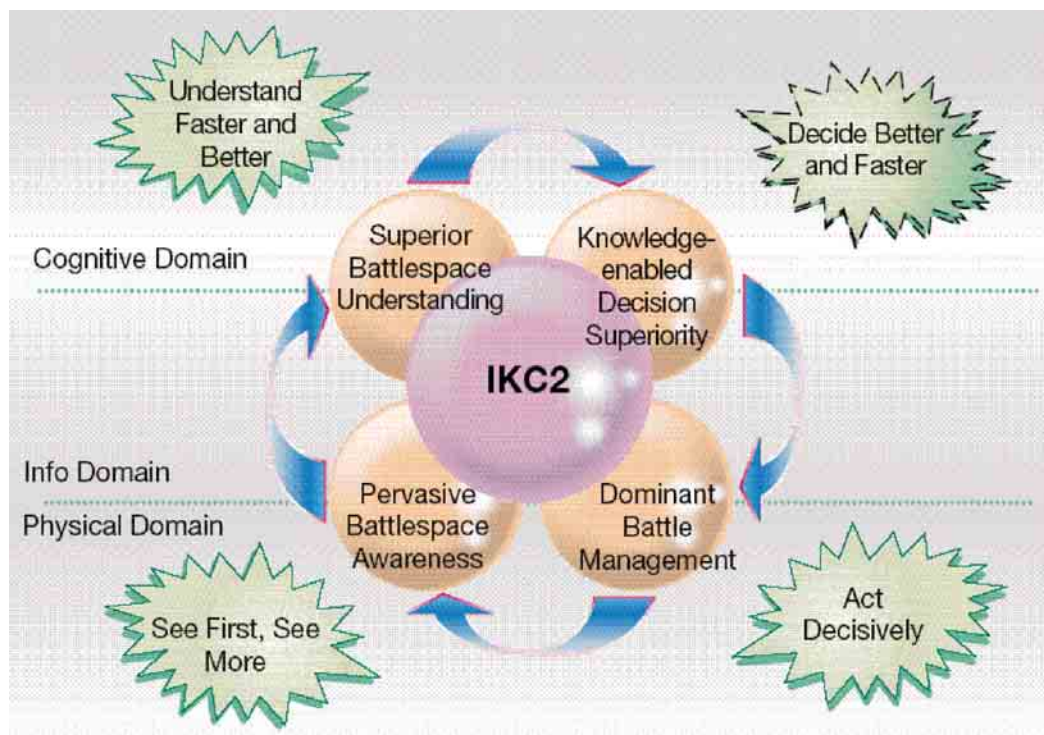

Figure 2. SAF's Integrated Knowledge-based Command and Control Framework
[Extracted from Ravinder Singh, et al, "IKC2 for the SAF – Organising around Knowledge", in Realising Integrated Knowledge-based Command and Control, Pointer, Monograph No. 2, (2003), p14.]

The Way Ahead

It is not an easy task to embark on the transformation journey and ensure the success of the IKC2. Initially, adherence to standards and requirements under the IKC2 framework will possibly slow down the current pace with which individual systems and capabilities are fielded.[54] What then are the main considerations and ingredients needed in this "salad bowl", in order to create and achieve NCW and IKC2 Capabilities?

As mentioned earlier, one of the key ingredients in achieving IKC2 is about *culture and people*. This is often cited in many reports of change but to really transform and harness the power of IKC2, the need for the shared purpose cannot be ignored. The development process, as argued previously, will take a long time. Few, if any, could afford the kind of resources and capital devoted to the transformation and NCW developments that the U.S. DoD has done. The SAF, with limited resources, would need to work out an overarching set of capabilities that our forces would need to possess.

The time factor highlights further the need to have the shared ownership of this journey. The hype of a technologically enabled transformation could quickly fade if the momentum cannot be sustained. The operations tempo will not be reducing due to the wider spectrum of operations that the SAF has to handle. Hence, commanders must set priorities so that work objectives are narrowed down to a manageable level. With the commitment of the leadership across the services, officers and men alike will feel that they are part of this transformation process, rather than being casual observers.

Hence, it must be clear to the commanders and warfighters why and what are we changing to induce understanding and develop commitment. With this, there is a need for a credible communication plan. The military people have shown tremendous capacity to adapt and are very good at a task-oriented kind of environment. The switch to having rigorous debate, discovery and experimentation among warfighters, defence academic and defence scientists will entail a different learning climate. The SAF Army's effort towards grasping the fundamentals of organisational learning at various command levels and training schools will support this effort. The Navy and the Air Force have also embarked on similar initiatives. A spirit of learning and sharing that transcends the services and right to the smaller units and teams will create the capacity to change. The challenge is how to make this become an integrated effort since IKC2 is very much about integration.

The second ingredient involves the difficult aspect of *structures and processes*. To be able to fight in an integrated manner and across a spectrum of operations, the issue of "jointness" needs to be carefully addressed. The need to be modularised and be task force oriented for better responsiveness and agility are already quite well accepted. However, what this entails in terms of being able to fight in an integrated manner and for commanders to have superior C2 in operations may not be that simple.

The faster and more complicated war becomes, the more the need for tighter and continuous cooperation among the services.[55] With a tight defence pie, the synergy can be obtained by having the joint staff channel the competitive environment among the services towards a productive purpose. There is a need to have flexibility and versatility to achieve operational success. Decision-making needs to be decentralized through understanding of the superior commanders' intention. IKC2's network structures contrast with the hierarchical nature of the SAF structure and a major revamp may be needed.

"Jointness" is intimately related to the information revolution since seamless information and knowledge interaction will not be bounded by divisions among the services. Our network-centric forces must be able to "plug" quickly into an integrated battlefield operating system and this will require interoperable communications, standards, doctrine, tactics and procedures. However, joint interoperability is quite different from coalition interoperability. With the SAF playing an increasingly significant role in U.N. peacekeeping operations and participating in numerous bilateral and multi-national exercises, a related consideration would be the issue of interoperability.

Activities that are important to adopting process changes include clarifying the new operating concept, developing new training methodologies and system, and taking on an experimental approach. The setting up of the SAF's Future Systems Directorate is a commitment towards transformation by focusing on exploring new operational

Exercise Forging Sabre: A step towards 'Jointness'

concepts and experimentation. However, such exploration would still require the active participation of commanders and men so that they can feel the tempo of change. It should not be taken as a validation exercise by troops and the emphasis must be that it is "*safe to fail*", a significant change in the mindset of military personnel. Experiments and lessons learnt from operations or exercises can be the source of emerging doctrine, or else there will be significant lags in doctrine development.

In fact, in order to have some creativity necessary to embrace NCW, IKC2 and effects-based planning, a "*dare to experiment*" attitude would enhance the process of adapting and learning. Likewise, while training evaluation and validating doctrines are necessary activities, a fresh look at the training process will be fruitful. This would include new learning methodologies (e.g. knowledge-based approach, experiential and team learning, adaptive thinking) and new doctrines (e.g. fighting integrated and joint). With such an approach, some of the major obstacles related to C2 development like information overload (especially in HQs) and the lack of bandwidth to mobile troops, can have more emphasis. The danger of relying on higher HQs having the best situational awareness could result in high-level commanders trying to be involved in minor tactical manoeuvre and operations. Situational awareness must also filter to the lower levels of command.

The third ingredient is related to *products*. Here, **visible deliverables** become important to sustain the transformation journey towards IKC2.

Products that are based on integrated C2 architecture will give the SAF a quantum leap in capabilities when combined with battlespace awareness and precision strike. Products for the tactical levels cannot be ignored and while operating in wireless mode for mobile forces still present significant technical challenges (e.g. bandwidth and reliability), intermediate products have to be tested so as to enhance the learning curve. Service commanders need to grasp the implications of being able to operate in an integrated manner and operating with new technologies will enhance the understanding of C2 requirements in the information age.

Products, while needing to leverage on technology, can also be in the form of learning from the experimentation process. This would also help develop the key competencies required to be familiar about operating in a networked environment. An overarching architecture needs to be developed and communicated quickly so that integration can at least begin to take shape, even though changes and fine-tuning to the architecture will be expected. However, experimentation and products inevitably imply the commitment to put in capital investments. Also, the more we rely on information resources and systems, the greater must be our efforts to protect them.[56]

Ultimately, investing in IKC2 as part of force transformation will have an impact on resources and on efforts tied to force readiness and near-term force development. The children of today are acquainted with playing computer games and are hence good at "button-pressing" to shoot at "enemies"

while playing a combat game. The "transformer" toy that allows them to change the form and shape of a robot to another more powerful version by just a few twists and add-ons is also very popular. However, military operations have become more complex and transformation will require more than just a few quick twists. Indeed, arguments have been raised regarding the possible vulnerabilities (e.g. easier to attack and exploit an integrated network, new innovations by adversary, inherent chaotic nature of operations) of having IKC2. There are also implications for soldiers relying too much on technology since machines as yet cannot match the judgment capability of human minds. The "champions" of the IKC2 journey need to be aware of such possible pitfalls.

Conclusion

In the past decade alone, we have seen tremendous development in the use of information technology for military peacetime information systems and wartime command and control systems. The security environment today has a reduced distinction between war and peace since peacekeeping, homeland security and war against terrorists have shown that the military need to adapt to performing in a spectrum of operations. While the development and acquisition of hardware will continue, the opportunity is there to move ahead by a fundamental shift towards networking of forces and capabilities.

The networking paradigm is inevitable in the future. Network-centric warfare and network-centric operations are not ends in themselves. Effects-based operations encompass the mind with focus on the mission and the conditions of military operations while NCW provides the framework and tools. They deal with the why, what, how and support of military operations, which are crucial in looking at the military transformation journey.

There is little doubt that the concept of integrated command and control under the context of the SAF's IKC2 framework can fundamentally change the way we train and fight. It is *real* in that it necessitates the commitment and capacity to change, as transformation is inevitable. This will enable commanders to operate in an ever-changing environment and where the spectrum of operations will require new command and control tools and processes. However, there are major impediments that must be tackled before IKC2 can succeed, or else the journey would remain a *myth* to many. These include the need to transform the **culture**, the **structure and processes**, and the ability to sustain support by having **visible deliverables**.

Amidst the excitement of exploring new ways to be able to fight in an integrated environment, core military imperatives will still be needed where the commander will discern the salient points pertinent to his mission and lead his men towards planning and operating successfully in combat. The possibilities with embracing NCW and integrated command and control are indeed tremendous. IKC2 provides the framework to redefine organizational structures and provide clarity to the orientation of C2 in the information age. If this can lead towards a SAF that

can deal effectively with threats across the entire spectrum of conflict, then the way ahead would need deliberate and continuous effort. ☺

Endnotes

1 Van Creveld, Martin, *Command in War* (Cambridge: Harvard University Press, 1985), p4.

2 David S. Alberts, *et al, Understanding Information Age Warfare* (CCRP Publication Series, Aug 2001), p131.

3 A.H.H. Manfred, "Information Age Command and Control – The Weakest Link?" (Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2002), p3.

4 A.K. Cebrowski and J.J. Garstka, "Network Centric Warfare: Its Origin and Future", *U.S. Naval Institute Proceedings* Vol. 124 No.1, (January 1998), p31.

5 David Potts and Jake Thackray, "No Revolutions Please, We're British", in *The Big Issue: Command and Combat in the Information Age*, ed. David Potts (U.K. Strategic and Combat Studies Institute, March 2002), p23.

6 Michael O'Hanlon, *Technological Change and the Future of Warfare* (Brooking Institution Press, 2000), p7.

7 This operation refers to the military objective by allied forces to degrade and damage the military and security structure that President Milosevic (Yugoslav President) has used to depopulate and destroy the Albanian majority in Kosovo. (From prepared statement of William S. Cohen, Secretary of Defense, to the Senate Armed Services Committee on 15 April 1999.)

8 Thomas D Young, "The Revolution in Military Affairs and Coalition Operations: Potential Problem Areas and Solutions" (US Monterey: Naval Postgraduate School RMA Paper, 24 July 2003), p1.

9 Andrew May, "Science forecasting: predicting the unpredictable", *Journal of the Defence Science*, Vol. 6 No. 2, (2001), p69.

10 *Creating the Capacity to Change: Defence Entrepreneurship for the 21st Century, Pointer* Monograph No. 1, (2003), pp2-3.

11 David Potts, "Tomorrow's War", in *The Big Issue: Command and Combat in the Information Age*, ed. David Potts (U.K. Strategic and Combat Studies Institute, March 2002), p23.

12 Ibid., p23.

13 This is the first sentence of the Executive Summary of the Network Centric Warfare, Department of Defense Report to Congress, July 2001, according to David S. Albers and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (CCRP Publication Series, June 2003), p98.

14 Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its origin and Future", *Naval Institute Proceeding* Vol. 124 No.1, (January 1998), p139.

15 Ibid, p3. An example was illustrated on how Wal-Mart achieve the competitive advantage by having a sensory grid of point-of-sale scanners which collect information and share them with the suppliers in near real time.

16 United States Department of Defense, *Network Centric Warfare: Department of Defense Report to Congress* (Washington, DC: Department of Defense, 2001), pv.

17 John J. Garstka, "Network-Centric Warfare: Increased Combat Power for Joint Military Operations", in *Realising Integrated Knowledge-based Command and Control, Pointer* Monograph No. 2, (2003), p48.

18 Arthur K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Future", *U.S. Naval Institute Proceedings* Vol. 124 No.1, (January 1998), p9.

19 Dan Caterinicchia and Mathew French, "Network-centric warfare: Not there yet", *Federal Computer Week*, (June 9, 2003), p3.

20 Ibid., p3.

21 Victor Davis Hanson, *Carnage and Culture* (Doubleday, New York, 2001), p19.

22 Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War* (CCRP Publication Series, Nov 2002), p1.

23 David A. Deptula, "Effects-Based Operations: A Change in the Nature of Warfare", *Defense and Airpower Series* (Arlington VA, Aerospace Education, 2001)

24 Ibid., pix.

25 Edmund C. Blash, "Network-Centric Warfare Requires a Closer Look", *SIGNAL*, (May 2003), p57. Blash contented that NCW is optimised for a lighter logistical "tail" component, hence it may not be suitable for all form of warfare..

26 Robert K. Ackerman, "Operation Iraqi Freedom: British Warfighters Exploits Network Centricity", *SIGNAL*, (Sep 2003), p33.

27 Australia wanted a pragmatic approach and sees this as being a mechanism for seeking a Joint capability focus. For more details, refer to: Ed Kruzins and Jason Scholz, "Australian Perspectives on Network Centric Warfare: Pragmatic Approaches with Limited Resources", *Australian Defence Journal* No. 150, (Sep/Oct 2003), pp19-33.

28 John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage", *SIGNAL*, (May 2003), p60.

29 David S. Alberts, *Information Age Transformation: Getting to a 21ˢᵗ Century Military* (Washington, DC, CCRP, June 2002), pvii.

30 Ibid., pp28-29.

31 Don M. Snider, "Jointness, Defense Transformation, and the Need for a New Joint Warfare Profession", *Parameters*, (Autumn 2003), p18.

32 Jason Sherman, "Requirement Revolution", *Defense News*, (4 August 2003), p1.

33 Ross Pigeau & Carol McCann, "Re-conceptualizing Command and Control", in *Canadian Military Journal* Vol. 3 No. 1, (Spring 2002), p62.

34 Ibid., p53.

35 David S. Albers and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, (CCRP Publication Series, June 2003), p14. They were referring to the definition by the U.S. Joint Chiefs of Staff Publication JSP Pubs. 1-02, Department of Defense Dictionary of Military and Associated Terms.

36 Ross Pigeau & Carol McCann, "Re-conceptualizing Command and Control", in *Canadian Military Journal* Vol. 3 No. 1, (Spring 2002), p54.

37 Ibid., p14.

38 Extracted from U.S. Department of Defense, *Dictionary of Military and Associated Terms* (Joint Pubs. 1-02)

39 William M. Connor, "Emerging Army Doctrine: Command and Control", *Military Review*, (March-April 2002), p80.

40 David S. Albers and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (CCRP Publication Series, June 2003), p17.

41 Ross Pigeau & Carol McCann, "Re-conceptualizing Command and Control", in *Canadian Military Journal* Vol. 3 No. 1, (Spring 2002), p56.

42 Definition was shown in their presentation to the Canadian Forces College on 18 Sep 2003 entitled: "A New Conceptual Framework for Command and Control".

43 G.E. Sharpe and Allan D. English, *Principles for Change in the Post-Cold War Command and Control of the Canadian Forces* (Kingston ON., Canadian Forces Leadership Institute, 2002), p4.

44 The OODA Loop was created by Lt-Col Boyd's observations on his own decision/action cycle as a USAF jet pilot fighting MIG-15s in the Korean War.

45 Jake Thackray, "The Holy Grail", in *The Big Issue: Command and Combat in the Information Age*, ed. David Potts (U.K. Strategic and Combat Studies Institute, March 2002), p26.

46 C4ISR (C4, Intelligence, Surveillance and Recognition) encompasses the entire sensors spectrum and how they are linked to provide intelligence and awareness.

47 Jake Thackray, "The Holy Grail", in *The Big Issue: Command and Combat in the Information Age*, ed. David Potts (U.K. Strategic and Combat Studies Institute, March 2002), p28.
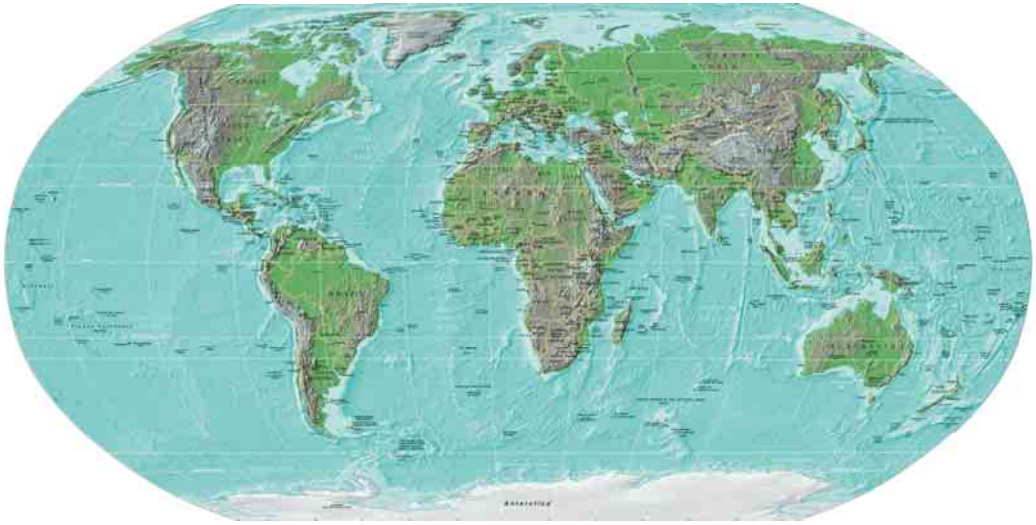
48 Ibid., p31.

49 David S Alberts, et al, *Understanding Information Age Warfare* (CCRP Publication Series, Aug 2001), p149.

50 J.N. Mak, *ASEAN Defense orientation 1975-1992: The Dynamics of Modernization and Structural Change* (Canberra: Strategic and Defense Studies Center, Australia National University, 1993), p162.

51 Ghazemy M Mahmud, "Top Brass Interview: Maj Gen Ng Yat Chung, Chief of Defence Force, Singapore", *Asian Defence Journal*, (7 & 8/2003), p14.

52 Ibid., p14.

53 Highlighted by the ex-CDF of SAF, Lt-Gen Lim Chuan Poh, in *Realising Integrated Knowledge-based Command and Control, Pointer* Monograph No. 2, (2003), p8.

54 *Realising Integrated Knowledge-based Command and Control, Pointer* Monograph No. 2, (2003), p10.

55 Pi S. Seet, "The Revolution in Military Affairs: Challenge to Existing Military Paradigms and Its Impact on the Singapore Armed Forces", *Pointer* Vol. 27 No. 2, (2001), p6.

56 Aaron E.S. Chia, "Countering the Friction and Fog of War in the Information Age", *Pointer* Vol. 29 No. 2, (2003), p117.

COL Lim Seng Hock is currently the Deputy Commandant and Chief Instructor of Singapore Command and Staff College, and concurrently Head of Training and Learning Systems Group in HQ TRADOC. A Signals Officer by vocation, he was formerly the Commander of Signal Institute and the Deputy Chief Signal Officer. He has attended the Army Command and Staff College Course in Australia and the Advanced Military Studies Course in Canada. COL Lim is an Overseas Training Award holder and he holds a Bachelor of Engineering (Mechanical Engineering) from the National University of Singapore, a Master of Science in Defence Technology from Cranfield Institute of Technology, U.K., and a Master of Business in Information Technology from Royal Melbourne Institute of Technology, Australia.

Globalization and Transnational Terrorism: Ironies, Interactions and Implications

by LTA Wee Wei Sheng, Edward

"***Osama bin Laden's al-Qaeda functions as a de-territorialized franchising agency for jihadist activity on a global basis – a Kentucky Fried Chicken of Global Terror. It operates through globalized religious, internationalist and 'normadic' networks.***"[1]

Introduction

Nearly a decade prior to the terrorist attacks against the United States on September 11, 2001, two eminent political scientists, Benjamin Barber and Samuel Huntington, made what would later seem prophetic statements about the nature of post-Cold War conflict. Barber wrote of a "Jihad vs. McWorld", where the "two axioms of our age – tribalism and globalism – clash at every point".[2]

Similarly, Huntington predicted a "Clash of Civilizations", whereby increased interactions between peoples "intensify civilizational consciousness and the awareness of differences between civilizations".[3] These views have fuelled the belief that the current wave of transnational terrorism is a backlash against the forces and effects of globalization, stemming from the fundamental incompatibility between secular, capitalist globalization and cultural, religious conservatism.

This oversimplifies the complex relationship between globalization and transnational terrorism. Moreover, it is also unhelpful to formulate effective counter-terrorism strategies. As such, this paper has three aims. First, it seeks to show that the current wave of transnational terrorism is not only a reaction against globalization, but is also paradoxically enabled by it. Second, it argues that current deficiencies in the globalizing international system acutely hinder counter-terrorism efforts. Third, it proposes that globalization provides essential motivations and avenues that aid the fight against terrorism, and which must be effectively harnessed. Clearly, it is impossible to analyze transnational terrorism as separate from globalization; both are intricately intertwined forces that characterize international security today.

Globalization and Transnational Terrorism Defined

Before exploring the multifaceted relationship between globalization and transnational terrorism, it is necessary to understand these often politicized and misinterpreted terms.

Globalization is a process rather than an outcome. It is best defined as "the expanding scale, growing magnitude, speeding up and deepening impact of interregional flows and patterns of interaction".[4] Today's "globalization" is a product of the 1990s. It followed the international collapse of communism and subsequent capitalist consolidation, as well as coincided with the digital Internet revolution and low-cost global communications. Modern globalization has taken place

in three forms: economic, cultural and political, each with its distinct features and effects.

Terrorism expert Bruce Hoffman defines terrorism as "the deliberate creation and exploitation of fear through violence against civilians in the pursuit of political objectives".[5] For most of human history, terrorism was traditionally confined to within national borders with specific state-centric objectives. What is more critical however, is the definition of the new "transnational terrorism". Transnational terrorism is terrorism that has transcended the confines of the territorially defined nation-state in terms of both its objectives and operations. Transnational terrorist groups are usually characterized by a universalist ideology, enhanced mobility and communication networks, multinational sources of recruitment and funding, and cross-border operations.[6] While Osama Bin Laden's Al-Qaeda network is the best-known example of a transnational terrorist group, other organizations such as Hamas, Hizbollah and the Liberation Tigers of Tamil Eelam have also displayed transnational features.

Globalization as a Motivation for Terror

Globalization is a critical feature of the context in which transnational terrorism has grown. Despite the tendency to view the current transnational terrorist threat as having religious inspiration, it is more accurate to see it as being motivated, at least in part, by the inequalities between nations as well as within them. Globalization has its fair share of "discontents"[7], while terrorists have always "aimed to exploit the

frustrations of the common people".[8] Globalization, in its various penetrative forms of westernization, secularization, democratization, consumerism and the growth of market capitalism, represents an onslaught to less privileged people in conservative cultures. They are certain that globalization is a US-led neo-imperialist conspiracy to threaten their traditions, religion and way of life, while bringing unfair distributions of wealth and power. Thus, the growth of disgruntled communities has proven to be the primary source of recruitment and support for transnational terrorists globally.

On the economic front, although globalization and the triumph of free-market capitalism was expected to usher in a new age of economic prosperity, a 1999 United Nations Development Program (UNDP) report stated that contemporary economic globalization was "partially responsible for an accelerating gap between rich and poor states, as well as between peoples, in the global economy".[9] In addition, the wealthiest oil-producing states of the Middle East are plagued by domestic economic inequalities. In 1997, Saudi Arabia reported a male unemployment rate of 46 percent[10], while *The Economist* reported in April 2000 that $4 billion out of the $7 billion windfall of unexpected oil revenues in 1999 disappeared in a "bonanza of unbudgeted expenditure".[11] Osama bin Laden has used this to his advantage, condemning the Saudi government and alluding to "the deterioration of the economy, inflation and ever increasing debts" in his *fatwas*.[12] In addition, neo-liberal economic reforms imposed on developing countries through the World

Bank and International Monetary Fund included the dismantling of public welfare programs that removed safety nets for the poor. In Egypt, for example, the *intifah* (market liberalization) has led to a sizable growth in poverty along with a rise in the wealth of a few.[13]

Cultural globalization has made images of Western life and the transmission of Western values ubiquitous across the world through the media and the Internet. Benjamin Barber argues that globalization is leading to a homogenized "McWorld" where American popular culture and consumerism is overtaking the globe.[14] Rejecting perceived cultural domination, conservative elements of society revile this as an attack on religious teachings and cultural traditions, and are generating movements of resistance, including support for transnational terrorism.

Finally, terrorism can most importantly be traced to a fundamental motivation – the struggle for power. Political globalization has extended US supremacy and interests worldwide, forming strong alliances with national governments, including undemocratic and oppressive ones. The need to protect its strategic interests also obliges the US to extend its military might internationally, not least establishing bases in the Middle East to protect the strategically important Persian Gulf. To extremists such as Osama bin Laden, the US support of oppressive regimes and the presence of US forces in Saudi Arabia, traditionally seen as sacred land, are unacceptable and need to be vigorously resisted by any means. To him, "there is no more important duty

than pushing the American enemy out of the holy land".[15] Therefore, to the extent that the economic, cultural and political dimensions of the US-led global order impinge upon and undermine Middle Eastern and/or Muslim ways of life, or at least are seen to do so, it elicits from militant Islamists and their supporters violent responses framed in the idiom of jihad.

September 11, 2001: The attack on World Trade Centre

Globalization as an Enabler of Terror

Although transnational terrorism in many ways represents a backlash against globalization, this is an oversimplification. The relationship between globalization and transnational terror is a paradoxical one. Transnational terrorism is "an authentic product of the globalized world and yet in fundamental conflict with it".[16] While it aims to repel US-led globalization, terrorism has concurrently harnessed globalization's features in three primary ways, through the exploitation of: new technologies; global financial networks; and reduced barriers to cross-border interactions. Al-Qaeda, in particular, has adapted so well to globalization that it has been called the MNC of the terrorist world with

its leader Osama bin Laden operating as "Terrorism's CEO".[17] In this context, globally connected networks facilitate the recourse to asymmetric attacks and are thus key enablers of transnational terrorism. Modern transnational terrorism is therefore especially dangerous because of the power that it derives from globalization.

First, globalization has enabled transnational terrorism through the exploitation of new technologies. The age of globalization has been the age of the Information Revolution – "the revolution in computing, telecommunications and data-transference capabilities".[18] The use of technological advances such as the Internet, mobile phones and satellite telecommunications has led to increased efficiency in terrorist-related activities and extended the global reach of terrorist groups. The global information age enhanced terrorist planning and coordination of operations, recruitment of potential members, communication among adherents, and attraction of supporters across national borders and long distances. As such, terrorist activities are no longer confined to territorially bounded regions, and now enjoy an expanded range and impact of operations. A case in point is the lethal impact and operational complexity of the synchronized attacks on New York and Washington by Al-Qaeda on September 11, 2001, which would not have been possible without the revolution in information technology. The Internet is also used clandestinely, including for passing encrypted messages embedded in invisible graphic codes through steganography.[19] Indeed, in 2000, former FBI Director Louis Freeh informed the US Senate that "untrackable encryption

is allowing terrorists to communicate about their criminal intentions without fear of outside intrusion".[20]

The reliance on advanced telecommunications networks has defined the organizational structures of transnational terrorist groups. These groups share the principles of networked organizations – horizontal rather than vertical organizational structures, decentralization of authority, and loose lateral ties amongst dispersed groups.[21] The desegregation of organizations has primarily been enabled by the lowering of communication costs for coordination. In particular, Al-Qaeda has effectively harnessed the networked structure in order to remain operational in the post-9/11 security environment. It became an umbrella organization with linkages to 24 Islamist groups, with members drawn from 48 countries and activities in 98 countries,[22] and has delegated many responsibilities to Islamist movements operating under its umbrella. This has made Al-Qaeda extraordinarily difficult to track and shut down. In addition, networks have also enabled terrorist groups across regions to rely on one another for technology, expertise and resources. Thus, the level of interconnectivity between terrorist groups has increased, even between those of different aims or ideologies.

Second, integrated global financial networks are a key supporting mechanism for the funding and operations of transnational terrorist groups. In a study of the economics of terrorism, Loretta Napoleoni exposes a "New Economy of Terror", a fast-growing system of terrorism-related economic activity, with a turnover of $1.5 trillion or five percent of the world's GDP.[23] This is a product of successful economic globalization in achieving deregulation, openness, privatization and integration in the world economy. In particular, features which have been exploited and adapted by terrorist organizations are integrated financial markets and the "digitization of money",[24] which facilitate the instantaneous transfer of funds across borders. Furthermore, financial globalization limits the level of control that governments have over financial matters, since the huge volume of transactions that occur on a daily basis, worth more than $1 trillion,[25] makes tracing terrorist funds extremely difficult.

The internet and integrated financial networks have eased terrorists' interactions and transactions across borders

Transnational terrorist organizations are broadening their reach in garnering financial resources. They have global financing networks that include legal non-profit charities and businesses, as well as illegal activities such as drug smuggling and kidnapping. Terrorist organizations like Al-Qaeda benefited from multi-million dollar businesses such as Al-Barakaat, a Somali-based international financial conglomerate, from which it received a five percent cut of annual profits, equivalent to about $25 million annually.[26] They

were also successful in manipulating global financial markets for their own gain. Investigations confirmed that Al-Qaeda succeeded in utilizing insider trading instruments to speculate in stocks and commodities markets prior to September 11th. It thus managed to attack the world's only superpower, and also made a fortune in the process. Moreover, when its strongholds in Afghanistan and Pakistan came under threat from US forces, Al-Qaeda scattered its financial resources throughout the world instantaneously. Money was laundered through US and European banks or converted into commodities such as gold, diamonds and even tanzanite, and hidden in far-flung locales in Sierra Leone and the Congo.[27] The integrated global economy thus provides transnational terrorist groups the opportunity to accumulate wealth and the ability to redistribute it quickly, all under the cloak of anonymity.

Finally, globalization enables transnational terrorism through the general lowering of barriers to cross-border interaction. With globalization, physical and commercial barriers have become increasingly permeable in order to facilitate trade and migrant movements. Open borders and visa-free travel policies have become commonplace. For example, the European Union (EU) has instituted open borders within member states. This is ideal for smooth flows of trade and manpower, yet it also allows terrorist organizations to easily establish cells across Europe and for operatives to move across borders virtually undetected. The sheer increase in world trade volume, particularly within free trade zones such as the North American Free Trade Area (NAFTA) and the EU have also made it much easier for terrorists to smuggle weapons or explosives across borders. Of the eighteen million cargo containers that arrive by sea each year in the US, only two to ten percent can be screened or searched.[28]

Globalization as an Obstacle to Counter-Terrorism

Whilst transnational terrorist groups have benefited significantly from the range of new capabilities afforded by globalization, globalization concurrently impedes the ability of nation-states to fight terrorism effectively. The international system has failed to keep up with the process of globalization and now suffers from serious regulatory and jurisdictional deficiencies.

A core concept of the international system that has been challenged by globalization is the traditional understanding of state sovereignty, a territorially-defined concept that gives states the exclusive authority to rule within their own borders.[29] Scholars such as Stephen J. Kobrin have argued that "globalization represents a fundamental change in the mode of organization of the world economy and world politics that compromises territorial sovereignty",[30] due to "deep integration"[31] of financial and informational flows which have made state-based jurisdiction difficult if not impossible. For example, a product of globalization that exists in the transnational and non-territorial sphere is the Internet. The prevalence of electronic commerce and communications weaken the abilities of the sovereign state to track, locate and prosecute illegal activities in cyberspace.

The transnational nature of electronic transactions also begets jurisdictional conflict, involving questions of overlap and ambiguity as to whether jurisdiction should be based on nationality, location or other factors. What is clear however, is the difficulty in applying traditional, territorially based jurisdictions to inherently non-geographical electronic transactions. Furthermore, sovereignty impedes counter-terrorism efforts through the rule of non-intervention in the domestic affairs of sovereign states. This hampers the investigation and pursuit of transnational terrorist groups that inherently operate across borders and judicial boundaries, and is reliant upon full cooperation between national governments which, until the declaration of the US-led Global War on Terror, was either unenthusiastic or completely absent. Even today, some national governments are still hesitant in handing over their nationals to the US for investigation or in prosecuting them for terrorism-related crimes.

Yet, the reluctance of states to partially surrender their sovereignty is understandable due to the fundamental weakness of laws and institutions at the international level. Even though the latter half of the twentieth century has seen the increasing use of international organizations, institutions and processes, global governance still leaves much to be desired. In terms of being able to deal with terrorism, international laws and institutions are especially vague and weak. Although there are clear, internationally recognized laws of war that are embodied in international treaties such as the Geneva Conventions of 1949, it is unclear if such laws apply to counter-terrorism campaigns. Such

operations are "different in important respects from what was originally envisaged"[32] in the laws of war, and there is disagreement especially as to whether terrorists should be legally treated as combatants and enjoy protective rights. During its campaigns in Afghanistan and Iraq, this lack of legal clarity allowed US refusal to recognize captured irregular forces as combatants, to prevent "terrorist organizations and their supporters to promote the legitimacy of their aims and practices".[33] This led to the indefinite confinement of suspected terrorists in Guantanamo Bay, an action that has incurred the wrath of human rights groups. In addition, out of the twelve multilateral counter-terrorism conventions that have been signed since 1963, none of them deal with transnational terrorism as a whole, and only one – the UN *International Convention for the Suppression of the Financing of Terrorism*, declared on December 9, 1999, directly deals with issues pertinent to transnational terrorism in the age of globalization.[34] After September 11, the UN rightly moved to draft an *International Convention against Terrorism* to form a comprehensive body of international law that addresses all legal aspects of modern transnational terrorism.[35] Unfortunately, yet unsurprisingly, the drafting committee has failed to progress beyond agreeing on a definition of terrorism.

International institutions share the deficiencies of international law. Despite the fact that covert activities by transnational terrorist groups such as money laundering and arms trafficking are criminal acts under international law, global law enforcement instruments

have played little if any role in the fight against global terrorism. Other than pursuing the terrorist groups themselves, tackling the international criminal network that sustains terrorism would be a logical counter-terrorism strategy. Unfortunately, the International Criminal Police Organization (INTERPOL) has been ineffective in dealing with transnational terrorism. It lacks US support and has often been harshly criticized in Congress and by Administration officials.[36] INTERPOL is also inherently weak in dealing with terrorism because historically it adopted the view that terrorism was political rather than criminal in nature, and its constitution was designed to preclude involvement in such areas.[37] Indeed, there is an extreme paucity of international institutions or agencies capable of addressing the transnational terrorist threat. The establishment of the International Criminal Court (ICC) in The Hague would be an ideal platform for the prosecution of international terrorist suspects, just as international tribunals have been formed to bring genocidal dictators such as Slobodan Milosevic to justice. Unfortunately, the effectiveness and relevance of the ICC has thus far been dealt a fatal blow due to US refusal to participate. Furthermore, a directory of counter-terrorism agencies by terrorism experts Graeme Steven and Rohan Gunaratna shows that compared to the 32 domestic counter-terrorism agencies in the US alone, there are only four international organizations involved in counter-terrorism.[38] Of these, two are regional organizations – the Inter-American Committee Against Terrorism (CICTE) and the North Atlantic Treaty Organization (NATO), and only two are truly international – the UN Terrorism Prevention Branch (UN-TPB) and INTERPOL, both of which have had limited impact on the current fight against transnational terror.

Source: dhs.gov

US Department of Homeland Security was created after the 9/11 incident

Globalization as a Weapon against Terror

In spite of the obstacles posed by globalization to counter-terrorism efforts, the mechanisms of globalization can and must be exploited to thwart the globalization of terror. Transnational terrorism is inherently a global problem. Thus, this paper proposes the following policy recommendations, which utilize the forces of globalization to combat transnational terrorism. First, integrate counter-terrorism tools between states to fully utilize intergovernmental networks in order to achieve maximal cooperation, including strengthening and supporting international laws and institutions. This would present a truly global front against transnational terrorism. Second, fully utilize globalization as a tool for equitable and sustainable economic development.

This would significantly decrease support for transnational terrorist groups who manipulate latent feelings of inequality and economic deprivation.

Transnational terrorist groups understand the interdependencies of the tightly integrated global economy. Similarly, countries around the world should have now realized that as long as they play a part in the global economy, no state is immune from the negative effects of transnational terrorism, neither can they tackle it alone. This should provide overwhelming incentives for states to cooperate in formulating a multi-pronged global response to terrorism – a truly integrated and multifaceted approach that combines cooperation and coordination in diplomacy, law, economics, finance, law enforcement, intelligence, etc. Such integration can be enabled by harnessing and strengthening existing intergovernmental linkages, which are themselves products of globalization. Globalization has reduced the barriers to international cooperation by starting to dissolve the absolutes of traditional sovereignty, including the idea that territorial borders alone define authority. It has already succeeded in getting states to cooperate in strengthening international economic laws and institutions. The success of the World Trade Organization should be an example of what can be achieved if the same level of international collaboration is replicated in the area of international security and counter-terrorism. Terrorists from around the globe have cast aside their national affiliations to wage war on the civilized world, it is time for nation-states to set aside narrowly-defined national interests and put up a robust multilateral response against the menace of transnational terrorism. Only then can both national as well as international interests be served.

The best means of integration to fight terror are international laws and institutions. In response to transnational terrorism, individual nations have already enacted powerful domestic legal codes such as the US's Patriot Act. The Patriot Act was the world's first financial counter-terrorism measure, recognizing that money laundering and a lack of financial transparency have facilitated the financing of global terrorism. It targets areas of the financial system believed to have been exploited by terror groups by preventing US firms from doing business with shell banks – banks registered offshore without a physical presence, and reinforcing the "know your customer" requirement, whereby the exact identity and background of anyone wishing to open a US bank account must be known.[39] However, because many other countries in the world do not have such legislation, terror money has simply flown elsewhere, especially to Europe. As such, similar legislation must be enacted at an international level, to ensure that terrorist manipulation of the international financial system is completely prevented. Similarly, an international institution or terrorism-fighting agency should be established and empowered, whose purpose would be to coordinate investigation, intelligence and jurisdiction of transnational terrorist activities. Globalization must be thus used as an advantage rather than an obstacle in counter-terrorism.

FBI's "Most Wanted Terrorists" list

Globalization can and must also be used as a driver for promoting equitable global economic development. There needs to be a "vision of sustainable development"[40] which includes economic growth, access to social needs such as education and health, and good governance, particularly in the Middle East and other Muslim states that have been neglected by the current wave of globalization. There is strong statistical support for the assertion that globalization reduces poverty. World Bank data shows that the percentage of the world's population that live in extreme poverty – less than $1 a day – has fallen from 31 percent to 20 percent since 1980.[41] Thus although growing inequality between rich and poor countries show that the poor may be relatively worse off, they are in fact better off in absolute terms.[42] Economic development removes an incentive or motivation to engage in transnational terrorist incidents, especially since many policy makers and scholars believe that "poor economic conditions create terrorist breeding grounds".[43] Additionally, unemployment, instability and poverty are also often associated with states either unwilling or unable to take decisive action against terrorists within their borders, like failed states such as Afghanistan.

In support of the link between development and terrorism, a statistical analysis of the effect of economic globalization on the number of transnational terrorist incidents within a sample of 112 countries from 1975 to 1997 found that "the economic development of a country and its top trading partners reduces the number of terrorist incidents inside the country".[44] Although this study does not clearly establish the causal relationship between increased economic development and decreased terrorist incidents, it certainly gives hope to the prospect that economic development has an important role to play in the fight against terrorism.

Conclusion

The relationship between globalization and transnational terrorism is one that has not been explored traditionally, nor has it been a principal consideration in current counter-terrorism efforts. This paper has set out to depict the complex relationship between two of the defining features of our world today, as well as suggest policies whereby globalization can aid the fight against transnational terror. Clearly, globalization fundamentally changed the nature of terrorism by being a key motivator and enabler of transnational terrorism. Globalization is a double-

edged sword – it both fragments and integrates, a phenomena James Rosenau terms "fragmegration".[45] Thus, just as it facilitates transnational terrorism, globalization can be used as a weapon against it. Transnational terrorism is inherently global, and clearly a unified global response is required. Concurrently, globalization is only one aspect of the multi-faceted transnational terrorism, which must be comprehended through other perspectives such as history, politics, psychology and religion. Only when a comprehensive approach is applied, can this menace be finally defeated.

(Ed note: This essay was the first prize winner of the 2005 CDF Essay Competition)

Endnotes

1   David Martin Jones and Mike Smith, "Contemporary Political Violence – New Terror in the Global Village", in *Globalisation and the New Terror*, ed. David Martin Jones (Northampton MA: Edward Elgar, 2004), p10.

2   Benjamin R. Barber, "Jihad vs. McWorld", *The Atlantic Monthly*, (March 1992), p53.

3   Samuel P. Huntington, "The Clash of Civilizations?", *Foreign Affairs*, (Summer 1993), p25.

4   David Held and Anthony McGrew, "The Great Globalization Debate: An Introduction", in *The Global Transformations Reader*, ed. David Held and Anthony McGrew (Cambridge UK: Polity Press, 2003), p4.

5   Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p43.

6   Rohan Gunaratna, "New Threshold Terrorism", in *The Changing Face of Terrorism*, ed. Rohan Gunaratna (Singapore: Eastern Universities Press, 2004), pp18-29.

7   Joseph E. Stiglitz, *Globalization and its Discontents* (New York: W W Norton, 2003).

8   Audrey Kurth Cronin, "Behind the Curve", *International Security* 27, No. 3 (2003), p35.

9   Held, "The Great Globalization Debate: An Introduction", p28.

10   Henry M. Clement and Robert Springborg, *Globalization and the Politics of Development in the Middle East* (Cambridge UK: Cambridge University Press, 2001), p179.

11   Ibid., p180.

12   Osama Bin Laden, "Declaration of War against the Americans Occupying the Land of the Two Holy Places", PBS Newshour Online (1996) <http://www.pbs.org/newshour/terrorism/internationa/fatwa_1996.html> (18 November 2005)

13   Jamal R. Nasser, *The Migration of Dreams and Nightmares*, p4.

14   Benjamin R. Barber, "Jihad vs. McWorld", *The Atlantic Monthly* (March 1992), pp53-63.

15   Osama Bin Laden, "Declaration of War against the Americans Occupying the Land of the Two Holy Places", PBS Newshour Online (1996) <http://www.pbs.org/newshour/terrorism/internationa/fatwa_1996.html> (18 November 2005)

16   David Martin Jones and Mike Smith, "Contemporary Political Violence – New Terror in the Global Village", p10.

17   Bruce Hoffman, "The Emergence of the New Terrorism", in *The New Terrorism*, ed. Andrew Tan and Kumar Ramakrishna (Singapore: Eastern Universities Press, 2002), p35.

18   Kevin A. O'Brien, "Networks, Netwar and Information-Age Terrorism", in *The New Terrorism*, ed. Andrew Tan and Kumar Ramakrishna (Singapore: Eastern Universities Press, 2002), p73.

19   Steganography is the embedding of messages in visual images, where the messages are disguised so that they cannot be seen by the naked eye. Ibid., p87.

20   Ibid., p88.

21   Michele Zanini, "The Networking of Terror in the Information Age" in *Globalisation and the New Terror*, ed. David Martin Jones (Northampton MA: Edward Elgar, 2004), p162.

22   Rohan Gunaratna, "The al-Qaeda Threat and the International Response" in *Globalisation and the New Terror*, ed. David Martin Jones (Northampton MA: Edward Elgar, 2004), p53.

23   Loretta Napoleoni, *Terror Incorporated* (New York: Seven Stories Press, 2005), pxviii.

24   Quan Li and Drew Schaub, "Economic Globalization and Transnational Terrorism", *Journal of Conflict Resolution* 48, No. 2 (2004), p234.

25 Ibid., p234.

26 Loretta Napoleoni, *Terror Incorporated*, p165.

27 Audrey Kurth Cronin, "Behind the Curve", p50.

28 Ibid., p235.

29 James A Caporaso, "Changes in the Westphalian Order: Territory, Public Authority and Soverignty", *International Studies Review* 2, No. 2 (2000), p2.

30 Stephen J. Kobrin, "Globalization, Multinational Enterprise, and the International Political System" (unpublished manuscript).

31 Ibid.

32 Adam Roberts, "The Laws of War", in *Attacking Terrorism: Elements of a Grand Strategy,* ed. Audrey Kurt Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), p186.

33 Ibid., p193.

34 Graeme C. S. Steven and Rohan Gunaratna, *Counterterrorism: A Reference Handbook* (Santa Barbara CA: ABC-CLIO, 2004), pp209-216.

35 John MacFarlane, "Organised Crime and terrorism in the Asia Pacific Region: The Reality and the Response", in David Martin Jones and Mike Smith, "Contemporary Political Violence – New Terror in the Global Village", in *Globalisation and the New Terror*, ed. David Martin Jones, p249.

36 Michael Fooner, Interpol (New York: Plenum Press), pvii.

37 Ibid., p10.

38 Graeme C. S. Steven and Rohan Gunaratna, *Counterterrorism: A Reference Handbook*, pp217-252.

39 Ibid., p113.

40 Audrey Kurth Cronin, "Behind the Curve", p56.

41 Robert Wade and Martin Wolf, "Are Global Poverty and Inequality Getting Worse?", in *The Global Transformations Reader*, ed. David Held and Anthony McGrew (Cambridge UK: Polity Press, 2003), p441.

42 Ibid., 441. Robert Wade demonstrates this by explaining that, "The absolute income gap between a developing country with an average income of $1,000 a year, growing at 6 percent, and a developed country with an average income of $30,000, growing at 1 percent, continues to widen until after the 40th year". However, the population of the developing country are still benefiting from economic growth stemming from globalization.

43 Quan Li and Drew Schaub, "Economic Globalization and Transnational Terrorism", p236.

44 Quan Li and Drew Schaub, "Economic Globalization and Transnational Terrorism", p254.

45 James N. Rosenau, "Governance in a New Global Order", in *The Global Transformations Reader*, ed. David Held and Anthony McGrew (Cambridge UK: Polity Press, 2003), p223.

LTA Wee Wei Sheng, Edward is currently a Project Officer in G1 Army. A Field Engineer by vocation, he was formerly a Platoon Commander in 35 SCE. LTA Wee is an Academic Training Award (Overseas) holder, and he holds a Bachelor of Arts in International Relations and History from the University of Pennsylvania, USA.

Modern Peacekeeping Operations and its Implications on the Role of the Militaries in Asia

by LTC Ang Kheng Leong, Benedict

Introduction: Rise of Modern Peacekeeping

The most important function of the United Nations (UN), as encoded in the words of its Charter, is "to save succeeding generations from the scourge of war".[1] Yet, since the end of the Cold War, the 'new world order' that was much proclaimed to be has become the 'new world dis-order' that is testimony to increasing UN impotence. The cases of Somalia, Rwanda, Bosnia and Herzegovina, and Angola have taught the UN several sobering lessons on peacekeeping,[2] including: (i) That peacekeeping is impossible when there is no peace to keep, and that peace-enforcement and/or peace-building missions are required instead; (ii) That peace-building missions demand very different skill sets of UN troops; (iii) That intra-state conflicts are in fact more dangerous than inter-state conflicts, since non-state actors do not play by international accepted norms and regulations; and that (iv) More than acquiescence, UN members, especially the permanent members of the UN Security Council, must actively support any UN peacekeeping mission without diluting the international resolve with

opposing views or unilateral action (or inaction).[3] Due to UN peacekeeping failures in the 1990s, there has been a growing recognition that there is a need to do more to preempt the breakdown of peace that would lead to such breakout of wars. Increasingly, the UN and the international community feel the need to establish a new kind of peacekeeping force to aid peacekeeping and where there is no peace, to make and build peace. In this context, modern peacekeeping has evolved out of the failures of 'traditional' peacekeeping.

Why Did Traditional Peacekeeping Not Work?

Traditional peacekeeping was meant to keep the peace between states. Inherent in the traditional peacekeeping mission was the notion that state sovereignty is sacrosanct, and that any UN deployment must have the consent of the parties involved. The role of UN peacekeepers was to be an impartial force, designed to monitor the adherence of the terms of the negotiated peace. It was not mandated to impose any will on either party. Such a role for the UN peacekeeping mission was necessitated and indeed influenced by the US-USSR superpower rivalry that dominated the international agenda during the Cold War. Predicated on the primacy of the maintenance of international order and stability, UN peacekeeping missions were necessarily constrained.[4]

Such a traditional view of peacekeeping missions did not auger well for the complex scenarios that played out in the 1990s. The phenomenon of intra-state conflicts in the post-Cold War era had led to the call to do more. Peacekeepers were sent into conflict areas where there was no clear victory on either side of the warring parties, and where either side could be looking to capitalize on opportunities to gain the upper hand. There was likely to be little or no commitment to the seize fire and that the halt in violence was imposed by the UN. In other words, the deployments were not into areas where peace was established but where the peacekeepers were expected to create it.[5] In such situations, the peacekeepers were expected to work hand-in-hand with peace-builders to create a self-sustaining environment.[6]

From State Security to Human Security?

Essentially then, there is a fundamental shift in the understanding of 'sovereignty' at the international level. Traditionally, state sovereignty was considered to be sacrosanct and was not to be violated. This was the principle that protected small states in an anarchic world characterized by self-help and power politics. The sanctity of state sovereignty accorded the notion of equality to states in the international political system. However, since the end of the Cold War, there is an increasing tendency to question the sanctity of state sovereignty, and challenge it with the notion of human security. In essence, there is increasing momentum to the view that the sanctity of a state's sovereignty is conditional on the fulfillment of certain fundamental obligations, failing which the international community would not be obliged to recognize the rights of such a (failed) state. In this

context, it becomes the international community's right, and in fact obligation (and responsibility) to protect.[7] There is also the view that in situations of gross human rights violations, it is not only morally legitimate to intervene, but also legal.

Coercive Inducement a New Role for Modern Peacekeeping?

As a response to the challenges of modern peacekeeping, new concepts such as 'coercive inducement' have been championed to deal with the new phenomenon of complex conflicts. Coercive inducement is defined as "the judicious resort to coercive diplomacy or forceful persuasion by the international community in order to implement community norms or mandates vis-à-vis all the parties to a particular crisis".[8] Essentially, coercive inducement challenges the traditionally accepted norms of peacekeeping such as the need for consent of local affected parties, the need for impartiality of UN troops, and the constrained use of force, i.e., only in self-defense.[9] Concepts such as coercive inducement would propose a more generous and liberal interpretation of such norms, giving peacekeepers a greater degree of freedom and more latitude for action. In the process, the sanctity of state sovereignty is questioned, and ultimately diluted.

Complexities and Challenges of Modern Peacekeeping

Modern peacekeeping has been described as combining the roles of administrator, mediator, and guarantor.[10] The growing complexity for the modern peacekeeping mission is due in no small part to the widening range of UN missions, including election observation and organization, humanitarian assistance and securing safe conditions for its delivery, separation of combatants, disarmament, protection of human rights, mine clearance, military and police training, boundary demarcation, civil administration, refugee assistance, reconstruction and development, and maintenance of law and order.[11] While the demand for peacekeeping missions has been high, the necessary planning and management of such missions, both at the HQ and field levels, have not been developed at a pace that can keep up with the growing demands and complexities of new peacekeeping missions. Peacekeepers are essentially thrown into the deep end of such modern peacekeeping operations and are left to figure out for themselves the scope, authority, mandate, terms of reference, support, and sometimes even the very objective of the mission. As contended by Jim Whitman and Ian Bartholomew as the crux of the problem, "the lack of functional political-military machinery within the United Nations, to assist in the framing of resolutions under Chapter VI or VII and to manage any military aspects on their implementation and control, is a fundamental institutional gap that must be filled if the use of collectively sanctioned military measures is to be effective. For the UN, as for its member states, the institutional capacity to integrate military effectiveness and political legitimacy is fundamental".[12]

UN peacekeepers overseeing disarmament in Haiti (Mar 05)

Besides growing in complexity, the widening range of missions also means that each UN mission could have multiple objectives that may be in conflict with each other.[13] For example, in Cambodia, the pursuit of human rights violators was subordinated to the desire to hold elections while in Somalia, the hunt for those responsible for killing UN troops took priority over the goal of seeking peaceful settlements.[14] Peacekeepers are therefore required to balance between objectives, which may be difficult or sometimes even impossible.

UN peacekeepers providing evacuation assistance in Tyre, Southern Lebanon (20 July 2006)

Another complexity and challenge of modern peacekeeping is that the nature of conflicts in which the UN intervenes has changed. Whereas conflicts were essentially between states during the Cold War,[15] conflicts within states appear to be more widespread in the post-Cold War era. Such intra-state conflicts present scenarios which are often volatile, uncertain, and ambiguous. Given such new and demanding scenarios in which modern peacekeepers are expected to operate in, the peacekeepers are necessarily subjected to higher risks. As pointed out by Cdr. Ramzan Johari of the Malaysian Peacekeeping Training Centre, the characteristics of intra-state conflicts are akin to that of failed states, with dysfunctional police, penal and judiciary authorities.[16] Peacekeepers will also likely deal with warlords and militia that do not abide by internationally accepted norms and conventions on armed combat. In addition, the proliferation of small arms and the involvement of child soldiers add to the problem of identifying who the 'enemy' is.[17] Further complexity is added by the need to handle large numbers of internally displaced persons (IDP). As Findlay noted, "(a)lthough the best militaries are well disciplined, organized and resourceful, few of the new peacekeepers will have the flexibility and sensitivity (not to mention training and equipment) for handling in a foreign environment such delicate situations as crowd control or intercommunal violence".[18]

Implications on the Role of the Militaries in Asia

Given the complexities and challenges of modern peacekeeping, what are the implications for countries in Asia in general and for their militaries in particular? To answer this, it is important to understand the current

geo-political context in Asia. The geopolitical reality in Asia today is that there are still many conventional inter-state hot spots, such as between India and Pakistan, the Korean Peninsula, and the Spratly Islands, to name the major ones. In addition, many difficult relationships exist in the region, for example, China-Japan, China-Vietnam, Thailand-Myanmar, and North Korea with East Asia in general. It can thus be said that inter-state concerns and the potential for inter-state conflicts remain high on the security agenda of Asian countries. In many of these situations, the traditional notion of sovereignty lends stability. In other words, by reinforcing the sanctity of state sovereignty, and by the mutual recognition of the primacy of such a principle, countries in Asia are assured that there is at least a common understanding regarding what is acceptable state action in terms of intervention (or non-intervention, to be more precise) in another state's internal affairs. Conversely, by challenging the sanctity of the sovereignty of the 'state', Asian countries run the risk of undermining the stability of the region.

Thus, while support for traditional peacekeeping missions remain fairly strong from Asia (India, Pakistan, Bangladesh, Malaysia), there is likely to be less support for modern peacekeeping missions, especially if the deployments are to countries in the region. China, for example, is generally against UN-authorised use of force, and has always argued for the respect of state sovereignty and non-interference in internal affairs.[19] For China, the consent from the relevant governments and/or parties must be obtained before any peacekeeping mission is dispatched.[20] In addition, the UN must remain neutral, fair, and impartial, and must not get involved in the internal conflict of a country.[21] A similar view is held by India. For example, Lt. Col. Purushothaman from the Centre of UN Peacekeeping in New Delhi asserts that "(p)eacekeeping mandates must be predicated on the consent of the parties, the impartiality of the peacekeepers, the need to be non-interventionist".[22] Yet another country sharing similar views is Sri Lanka. In direct response to the Brahimi Report, Maj. Gen. Dipankar Banerjee noted that while genocides had to be prevented, issues of state formation and consolidation were real concerns in Asia, since most Asian countries had only recently gained independence through decolonisation. Thus, "(w)hile national sovereignty must not be used as a shield to mask the atrocities perpetrated by a state against its own citizens, any international action that violates the principle of state sovereignty must be founded on extremely solid ground".[23]

Given this then, the implication on the role of the military in Asia is obvious. Unless there is strong support at the political level for modern peacekeeping, Asian militaries are more likely to operate business as usual. Factors such as force structure, equipping, and training are a direct result of elite threat perception. As long as the threat to Asian countries remain conventional, it is unlikely that Asian militaries will devote scarce resources to train their troops for complex modern peacekeeping missions, especially if there exist the potential to drag troop-contributing countries into regional conflicts.

UN peacekeepers from China involved in de-mining in Lebanon (August 2006)

Yet, even while Asian countries are reluctant to get involved in complex modern peacekeeping missions, there is an extant moral pressure at the international level for countries to "do something", especially in situations where egregious atrocities have taken place. To better prepare for such situations, there is a recognition that troops need to be adequately trained to handle the unexpected, given that modern peacekeeping missions are radically different from conventional operations that the traditional soldier is prepared for. From tension diffusion tasks such as negotiation, mediation, and conciliation, to 'high intensity' peacekeeping tasks such as peace enforcement and armed escort of humanitarian aid, new skill sets are expected and required of UN peacekeeping troops.[24] Thus, militaries around the world, including those in Asia, would need to put in place some measure of training for troops committed for such missions. However, this does not mean that

militaries in Asia would be rushing into new forms of training for UN missions. To be sure, it seems unlikely that Asia is ready to fully commit to the effort that is required for this new reality. It is quite revealing that of the 27 peacekeeping training centers in the world, only one is in Asia (Malaysia). For all other Asian countries that send their troops for UN peacekeeping missions, they train their troops locally before deployment.[25] It can be argued that for as long as traditional security concerns dominate the security agenda of Asian countries, Asian militaries will continue to be concerned with building up and sustaining conventional orbats and structures to address more conventional threat scenarios.

Conclusion

The nature of conflicts has changed since the end of the Cold War. To the extent that when traditional methods of peacekeeping were used to handle such conflicts, they were grossly inadequate and the peacekeeping missions failed. As a response to such failures, the international community saw it necessary to redefine the scope of peacekeeping to be more expansive to include new roles such as armed protection of humanitarian aid, separation of combatants, disarmament, as well as new concepts such as coercive inducement. What this means for modern peacekeeping is that it has become more complex. The complication that arises out of modern peacekeeping is that it calls into question the sanctity of the sovereignty of the state, thereby undermining a key pillar of international order and

stability. As far as Asia is concerned, there are two broad implications for the role of the military. First, at the geo-political level, the commitment of forces for such new roles will reinforce the burgeoning norm that, at its heart, questions the sanctity of state sovereignty. This does not sit well with countries in Asia. Plagued by a multitude of conventional/ traditional security concerns, the mutual recognition of the sanctity of state sovereignty, an agreement to play by the same rules, has ensured a high degree of order and stability in Asia. By questioning the basis for order and stability in Asia, Asian countries will further complicate the task of managing the risk of the escalation of conflict. The second broad implication is that at the military level, militaries in Asia are largely structured for a "conventional" response, i.e., as a very specific response to a perceived threat in a traditional state-versus-state scenario. Modern peacekeeping requires a paradigm shift in the way armed forces are conceived to achieve the political ends. To be effective, this must be translated to concrete action such as equipping and training at the tactical level. However, the re-structuring of conventional forces in Asia for modern peacekeeping will surely be tempered by more real concerns, given the conventional scenarios that still loom over the Asia region. 🖳

(Ed note: This essay was the third prize winner of the 2005 CDF Essay Competition)

Endnotes

1   Brahimi, Lakhdar, Report of the Panel on United Nations Peace Operations, United Nations Document No, A/55/305, 2000, pviii.

2   Blagescu, Monica and Schnabel, Albrecht (eds.), Reforming UN Peace Operations: New Challenges for Peacekeeping Training (Tokyo: United Nations University, 2002), p40.

3   ibid., pp40-41.

4   Daniel, Donald C. F., and Hayes, Bradd C., with Oudraat, Chantal de Jonge, Coercive Inducement and the Containment of International Crises (Washington DC:US Institute of Peace Press, 1999), p9.

5   Brahimi, op. cit., pviii.

6   ibid.

7   This is in fact the basis for the Report of the International Commission on Intervention and State Sovereignty. See Evans, Gareth and Mohamed Sahnoun (co-chairs), The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty (Ottawa: International Development Research Centre, 2001).

8   Daniel and Hayes, op. cit., px.

9   ibid., pp24-26.

10   Findlay, Trevor (ed.), Challenges for the New Peacekeepers (New York: Oxford University Press, 1996) p18.

11   ibid., pp17-18.

12   Daniel, Donald C. F., and Hayes, Bradd C. (eds.), Beyond Traditional Peacekeeping (New York: St Martin's Press, 1995), p173.

13   Findlay, op. cit., p18.

14   ibid.

15   ibid., p22.

16   Blagescu, op. cit., pp54-55.

17 ibid.

18 Findlay, op. cit., p19.

19 Daniel and Hayes, Beyond Traditional Peacekeeping, op. cit., p123.

20 ibid., p124.

21 Findlay, op. cit., p100.

22 Blagescu, op. cit., p65.

23 ibid., p93.

24 Morrison, Alex (ed.), The Changing Face of Peacekeeping (Canada: Canadian Printco Limited, 1994), p159.

25 Shioguchi, Tetsuo, A New Approach to UN Peacekeeping Operations: Proposal for a New PKO Center (Tokyo: IIPS, 2001), p2.
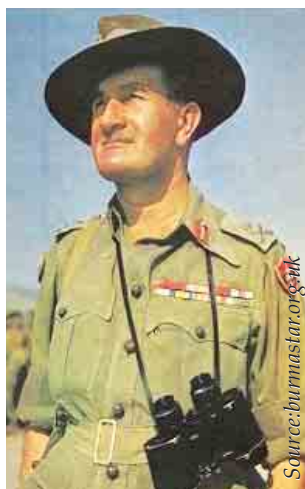
LTC Ang Kheng Leong, Benedict, is currently a Branch Head in Air Plans Department, HQ RSAF. A Pilot by vocation, he was formerly a Section Head in Air Intelligence Department and a Squadron Pilot in 140 Squadron. LTC Ang holds a Bachelor of Social Science (2nd Class Upper Honours) in Political Science from the University of Singapore, and a Master of Science (Strategic Studies) from the Institute of Defence and Strategic Studies, Nanyang Technological University.

Transforming an Army: Military Leadership and Military Transformation in the British and Indian Armies

by LTA(NS) Toh Boon Ho

Field Marshal Bernard Montgomery

General William Slim

"***...some [commanders] like Field Marshal Montgomery...were essentially egomaniacs [and] were quite incapable of working effectively with Allied military leaders and staffs. [Other commanders] inspired respect by the obvious force of their personalities and intellect: Field Marshal Brooke and General Slim, to mention two examples.***"[1]

The Second World War created a wellspring for the emergence of several outstanding military leaders on opposing sides of the conflict. Names like Yamashita, Rommel, de Gaulle, Patton and Montgomery easily come to mind. This study is focused on the examination of two particular leaders in the Commonwealth armies: Field Marshals Bernard Law Montgomery of the British Army and William Joseph Slim of the Indian Army.

Both leaders took over command of combat formations in 1942 which were reeling from defeat, on the defensive and suffering from low morale. By 1945, both Montgomery and Slim were at the apex of their operational military careers and presiding over confident, battle-hardened and well-equipped forces which had defeated their respective theatre enemies through greatly improved combat skills in the test of battle. The period between

1942 through 1945 witnessed the transformation of the British and Indian Armies in the field from mere novices to masters of their craft. Much credit for the transformation of both forces can be attributed to the leadership of both commanders as well as the ability of the system to undergo and manage change under the stress of continuing combat operations. This paper aims to study how the transformation of both the British and Indian Armies took place between 1942 and 1945 through an examination of the key factors of leadership; doctrine, training and morale in transforming the British and Indian Armies into effective combat forces that achieved victory over the Axis powers in 1945.

Military Leadership

Although both Montgomery and Slim belonged to the same military organisation, their leadership styles were diametrically different and elicited mixed reactions from those - their superiors and subordinates - who interacted with them. Montgomery was adored by his 8th Army soldiers and close followers. Following his assumption of command of the 8th Army in 1942, he became known to the British public as the ever-victorious general as he never lost a battle from that time onwards. However, Montgomery had an uncompromising and condescending streak which infamously, did not endear him to his American coalition partners and immediate superior, General Dwight D. Eisenhower, the Supreme Commander of the Allied Expeditionary Forces. The relationship between both men was at best professional; at worst, testy if not strained.[2]

William Slim was similarly adored by the men he led in the XIV Army in Burma. Commonly known as "Uncle Bill" to his men, he inspired not because he was known as the ever-victorious general, but because he triumphed in the face of defeat against the "invincible" Japanese during the dark days of 1942. In his words, "to be cheered by troops whom you have led to victory is grand and exhilarating. To be cheered by the gaunt remnants of those whom you have led only in defeat, withdrawal, and disaster, is infinitely moving – and humbling."[3] The crowning glory of his leadership was the transformation of the army he led from one of defeat into victory against the Japanese in 1944-45 during the reconquest of Burma. Unlike Montgomery, Slim got on well with his superior Admiral Lord Louis Mountbatten, Supreme Commander, Southeast Asia Command (SEAC)

Source: Robert Lyman, Slim, Master of War

"Uncle Bill" chatting with one of his soldiers

and more famously, with his coalition partner, the irascible American general, Lieutenant-General Joseph W. "Vinegar Joe" Stilwell, who was known to dislike the British deeply. In Slim, Stilwell found both mutual respect and admiration for Slim's leadership abilities in the face of extreme adversity and his professional conduct as a soldier during the long retreat from Burma in 1942.[4]

Narcissistic versus Level Five Leadership

In current management literature on leadership, one can discern between two contrasting styles of leadership: Narcissistic vs. Level Five Leadership. Narcissistic leadership is marked by charisma and the focus on the leader himself, the messiah who will deliver his followers from adversity by adhering to his great vision. Success was the result of the leader, and nothing else.[5] Level five leadership is the fundamental opposite. While focused on the individual leader, success is not so much attributed to the leader, but rather, by the leader to the synergistic teamwork and actions of his followers that enabled success to accrue to the entire corporate body. The role of the leader is merely to ensure that the team in charge shared the same management philosophy and pulled together in the same direction. Success would eventually culminate to the team. The level five leader does not see "me", but "them". He is humble, but tenacious. He undertakes responsibilities, takes the rap for failures but attributes success to his team.[6]

Narcissistic Leadership

Montgomery with his theatrics and an eye for positive public relations was an archetypal narcissistic leader. Not only did he possess a great vision, he also motivated the soldiers under his command. He turned them into his ardent followers by ensuring that his soldiers were always well-prepared for battle.[7] The result was well-trained and well-equipped troops who were committed to battle only when success was more than assured. This strategy guaranteed victory and raised morale. Montgomery also ensured that his formation commanders and staff were hand-picked by him as much as possible. He took and uprooted his staff wherever he went: From England to North Africa; to Italy and finally, Normandy. This was the only way to ensure that his will was imposed on his formations such that they became extensions of himself and could be trusted to do his bidding and followed his plans. Montgomery always maintained a tight grip on the battle by keeping his commanders on a short leash. In this way, he ensured that his command was thoroughly indoctrinated in his style of warfare.[8] He was also extremely competitive and sensitive to criticism. Despite the civilities in the relationship between him, Eisenhower and General Omar Bradley, Montgomery never did establish a good personal rapport with his American coalition partners.[9] All these characteristics did not impact negatively on Montgomery's leadership, however, and he retained the confidence of his patrons, Chief of Imperial General Staff (CIGS) Field Marshal Alan Brooke and Prime Minister Winston Churchill, as well as inspiring his soldiers to victory.

Monty observing his troops

Level Five Leadership

Unlike Montgomery, Slim was a relative unknown. In 1940, Montgomery was a rising Division Commander serving in France under the future CIGS.[10] Slim was only a Brigadier serving in Eritrea where a botched military operation almost cost him his army career.[11] Serving in Burma as a Corps Commander during the retreat in 1942, he was offered a poisoned chalice, but nevertheless played his cards well, despite being dealt a bad hand from the start. Rather than blaming everything and everyone except himself for the debacle they found themselves in, Slim was more introspective and circumspect. Slim was also particularly uncomfortable with narcissistic leaders like Major-General Orde Wingate and General Douglas MacArthur, who received few kind words in his memoir.[12] Unlike Montgomery who could not and did not tolerate mistakes, Slim was more forgiving. He was tolerant of failure as he recognised them as valuable lessons in command. Slim learnt from his mistakes.[13] It was well-noted that Slim was always unflappable despite being in the most desperate of circumstances.[14] If mistakes were made, even those which were not of his own doing, he gamely took the blame for it. He did not pin the blame on others, be it his superiors or subordinates.[15] As he reflected on the disaster in 1942 in his best-selling memoir, *Defeat into Victory*, Slim reproached himself for taking counsel of his fears and not choosing the bolder course of action when confronted with the dilemma of caution versus boldness.[16] Throughout the entire campaign in Burma, Slim was to be sent in when things were going badly. The retreat from Burma in 1942 and First Arakan in 1943 were notable examples. Through his actions, he was to retrieve some semblance of order and a positive outcome from a bad situation. Slim was the ultimate Level five leader: humble in defeat; tenacious in battle but gracious in victory.[17]

Doctrinal Shortcomings

Although both Montgomery and Slim exhibited different leadership styles, both agreed on one thing: they believed that the way to transform their own fighting forces into effective soldiers who could best their opponents in battle was not obtaining more material, but to focus on the basic elements of doctrine, training and morale in their respective commands.[18] The poor record of Commonwealth forces in battle against first-rate enemies like the Germans and Japanese between 1940 and 1942 was largely attributed by both Montgomery and Slim to a lack of proper training of their troops. Against second-rate troops like the Italians in 1940, both British Army and Indian Army troops, trained for warfare in the Western Desert were able to mask their organisational weaknesses and still triumph over their Italian enemies.[19]

When pitted against enemies with first-rate Generals and battle-hardened, experienced troops with offensive-minded doctrines like the Germans and Japanese, the Commonwealth armies' organisational deficiencies immediately became apparent. In the early days of the Second World War, the Commonwealth armies were out-trained, out-fought and out-thought by their enemies with disastrous consequences for their troops' morale and confidence in their leaders and organisations. Their doctrine was cumbersome and staid compared to the fluid pace of their enemies. There was no common doctrine to speak of. The British system was based on a contradictory dual system of command that at the operational level, comprised 'umpiring' and at the formation level, was represented by 'restrictive control'.[20] Too much leeway was given to field commanders to interpret doctrine in their own manner. Too much faith was placed on the British officer's ability to improvise successfully in any crisis.

Source: nla.gov.au

Tanks in action at El Alamein

Organisationally, their command and control systems could not keep pace with the rapid operational tempo of their enemies.[21] Much was needed to be done by both Montgomery and Slim to transform their theatre commands into combat effective forces that could defeat their enemies in battle.

Addressing Doctrinal Shortcomings

The doctrinal leeway afforded to senior British commanders paradoxically allowed the best commanders to interpret and stamp their own authority on their own commands. This had the effect of addressing and alleviating the doctrinal shortcomings of the Commonwealth armies which had become painfully clear in 1940 through 1942. Montgomery was well-known as a no-nonsense leader who expected a lot from his subordinates. He was quick to weed out officers whom he felt unsuitable for field commands.[22] He was apt to promote his protégés into positions of field command under his watchful eye. By having his faithful protégés in place, Montgomery ensured that his well-laid plans were executed by officers who had his trust and confidence. These were subordinates who subscribed to his way of war-fighting. Montgomery was therefore susceptible to having a big entourage of his loyal followers moving with him as he progressed through the leadership ranks during the course of the Second World War.

Key to Montgomery's interpretation of official doctrine was the need to maintain 'balance', which is the

maintenance of the initiative and the holding of sufficient reserves to deliver an unexpected blow to the enemy to keep him conversely unbalanced. Montgomery was the master of the set-piece battle, as he successfully proved at El Alamein and elsewhere in Italy and Northwest Europe. Though successful at driving back his opponents, Montgomery could never 'catch his opponents' and failed to exploit fully the successes he had achieved.[23] Montgomery could not match the doctrinal mastery and strategic flexibility of Slim. Slim not only mastered the set-piece battle as evidenced by the battle for Imphal-Kohima but also the master-stroke at Mandalay and Meiktila in 1944, where he exhibited his flair as a 'manoeuvrist general'.[24]

The battle of Imphal and Kohima in March 1944

Ever the Level five leader, Slim took his lessons wherever he found them. Slim subscribed to a simple principle of war imparted to him as a young officer cadet by an experienced sergeant-major: "There's only one principle of war and that's this. Hit the other fellow, as quick as you can, and as hard as you can, where it hurts him most, when he ain't lookin[g]".[25] Like Montgomery, Slim imposed his own interpretation of doctrine on his command. He profited from the experience of defeat at the hands of the Japanese in 1942 by ruthlessly exploiting the Imperial Japanese Army's organisational weaknesses of rigidity, lack of flexibility and all-too-predictable tactical conduct during operations to turn defeat into victory in 1944-45.[26] Slim similarly kept a tight grip on the battle situation by maintaining tight control over his subordinates. While Slim did not uproot his subordinates with him as he progressed up the command chain and disapproved of 'travelling circuses', he heavily relied on fellow regimental officers from the Gurkha regiment at each level of command that he served in. On both these counts, Slim was not unlike Montgomery.[27]

Both Montgomery and Slim were strong-willed leaders. Through their own interpretation of British and Indian army doctrine, both commanders imposed their will and personal interpretation of the existing doctrine and executed it through loyal staffs under their command. Combined with the marked improvements in the training and morale of the men under their command, coupled with the increasing material support made available by fully mobilised war economies, these factors enabled both leaders to overcome the continuing doctrinal deficiencies of their organisations.

Transforming an Army: Training and Morale

To remedy their organizational deficiencies, Montgomery and Slim focused on training. Morale was inextricably linked to training. With proper training and mastery of their environment, it was possible for the individual soldier to gain confidence in his soldiering skills and concentrate on defeating the enemy. Beyond training the individual soldier, training of the higher formation staff was also sorely needed at divisional, corps and army group levels. The success of Montgomery and Slim in the latter half of the Second World War can be attributed to the transformation of the training regime in both the Home Forces based in Britain and the Indian Army in SEAC.[28] A structured training system incorporating the latest lessons learnt in combat against the Germans and the Japanese were systematically disseminated and incorporated into the training syllabus in training formations. Regular updates from the combat theatres were disseminated through the promulgation of training memorandum in the form of Army Training Memorandum Training Notes from the operational theatres to training centres in the United Kingdom (UK) and in India.[29] In Burma, for example, following the First Arakan debacle in 1943, the radical decision was taken to remove two divisions from front-line service in July 1943 and convert them into training divisions to provide the institutional foundations for training a sufficient pool of jungle-schooled and well-trained replacements for the front-line units.[30] Priority was also placed on equipping and training the various formations for jungle warfare which were promulgated through the issuing of the Army in India Training Memoranda War Series and Military Training Pamphlets which were progressively updated and incorporated the latest lessons learnt from encounters with the Japanese.[31]

A major realization also took hold. The previously haphazard training standards which prevailed as a result of the laissez-faire attitude and leeway granted to British formation commanders had to be tightened through the introduction of battle drill at all levels: from individual fieldcraft, platoon and company drills, through to divisional and corps exercises which standardized training methods and allowed for interoperability of units which was hitherto absent. Drill also allowed the dissemination of a common doctrine which could be easily understood by all ranks. Training in the Home Forces in the UK, Montgomery's 8th Army in North Africa and Slim's XIV Army in Burma laid great emphasis on battle drill. With increasing attrition of experienced and battle-hardened officers and NCOs as the war wore on, an institutional response in the form of battle drill was needed to indoctrinate replacements.[32]

Both Montgomery and Slim also imposed their own interpretation of doctrine thoroughly throughout their own theatre commands. Battle drills were devised and imposed. Through carefully devised and rehearsed attack plans, their troops were slowly introduced to battle and blooded in sure-win, set-piece battles against their enemies. Great superiority in numbers was used against enemy positions: Brigades used against company positions; battalions

employed against platoon positions. In Slim's words, "if you have a steam hammer handy and you don't mind if there's nothing left of the walnut, it's not a bad way to crack it".[33] Montgomery employed similar methods. These local successes raised the morale of troops, increased the troops' faith in their leaders and developed confidence in their fighting methods.

The troops' morale was of paramount concern to the Commonwealth armies' leaders. The CIGS and the War Office in the UK, as well as theatre commanders like Montgomery and Slim were preoccupied with their troops' morale. A recent reassessment of Montgomery's methodical conduct in the 1944 Northwest Europe campaign concluded that his failure to exploit his successes there was largely the result of his over-riding concern to keep casualties low in order to preserve their morale. In addition, the 21st Army Group was the principal British combat formation in Northwest Europe and main contribution to the overall Allied effort to fulfil Britain's war aim of attaining victory and staking Britain's claim at the victory table. By the end of 1944, replacements from the UK began to run low. Desperate measures, including the disbanding of active divisions to provide trained replacements for the field formations, were being undertaken. Montgomery, ever aware of his dwindling manpower pool, could not afford risky manoeuvres that could cost him divisions he could neither afford to lose nor replace. He was also fully cognizant of the fragile morale of his conscript army. They had to be guaranteed victories or else their morale and combat effectiveness will plummet.[34]

Slim too, was concerned about his forces' morale. In particular, he had to debunk the myth of Japanese invincibility in jungle warfare, built upon their successes in Malaya, Burma and First Arakan. The only way to improve morale and his troops' confidence was to undertake specialist jungle training that made the British, Indian and African soldier confident and comfortable in the jungle.[35] Slim's efforts were well-supported by the Commander-in-Chief in India, Sir Claude Auchinleck, who upon his appointment in June 1943, immediately undertook a dramatic reform of the training policy and training institutions in India to support SEAC.[36] General Sir George Giffard, Slim's patron, took over responsibility for rear area administration and put in a first-rate performance. This act relieved Slim of administrative distractions and allowed him to concentrate on whipping his army into shape.[37]

Source: Robert Lyman, Slim, Master of War

Slim being knighted after his victory at Imphal in December 1944

Although Montgomery was an attention-seeker and actively sought publicity, he shared a similar genuine concern as Slim in communicating his ideas to the men under his command. Both Montgomery and Slim were great communicators in their own right. Both commanders made the extra effort to speak to the men in the field, in some cases, on the bonnet of a jeep. Montgomery too, made the effort to speak to every battalion under his command before the Normandy invasion in 1944. Both of them made their soldiers feel and understand the critical role they played in the great enterprise of war. They were able to distil complex ideas into simple messages that resonated with the men under their command. In this way, direct communications with the troops helped to sustain and increase their morale. Coupled with effective training and battlefield successes, it was a potent formula for uplifting their troops' morale.[38]

Monty at the Brandenburg Gate in Germany in 1945

Conclusion

Britain's victories in Europe and Burma in 1945 bear testimony to the successful transformation of the Commonwealth armies from defeat in 1940-1942 into victory three years later. The transformation was most pronounced in the two key field formations commanded by Montgomery in North Africa and Europe and Slim in Burma. While the increasing material made its presence felt towards the latter part of the Second World War, the key determinants of victory lay in the leadership of both Montgomery and Slim in transforming their hitherto defeated formations into well-trained and well-led forces that could beat their erstwhile invincible enemies in battle. Although the two commanders differed markedly in their leadership styles, both were in unison in their emphasis on doctrine, the crucial role played by battle drills and the importance of building up their troops' morale through specialist training and blooding them in successful battles which guaranteed victory. Through this virtuous cycle of training, successful battle introduction and victories, both Montgomery and Slim retained the confidence of their men in their leadership, their own fighting formations, and more importantly, their self-belief that they can beat their enemies totally and decisively in the field of battle.

(Ed note: This essay was the merit award winner of the 2005 CDF Essay Competition)

Endnotes

1   Gerhard L. Weinberg, *A World At Arms: A Global History of World War II* (Cambridge: Cambridge University Press, 1994), pp918-919.

2   Ibid., p444; Eisenhower privately remarked that, "Goddam it, I can deal with anybody except that son of a bitch". Cited in Rick Atkinson, *An Army at Dawn: The War in North Africa, 1942-1943* (London: Little, Brown, 2003), p466.

3   Field-Marshal Viscount William Slim, *Defeat into Victory: Battling Japan in Burma and India, 1942-1945* (New York: Cooper Square Press, 2000), ppxi-xii, p114.

4   Ibid., ppxii-xiii; Duncan Anderson, "The Very Model of a Modern Manoeuvrist General: William Slim and the Exercise of High Command in Burma", in *The Challenges of High Command: The British Experience*, ed. Gary Sheffield and Geoffrey Till (Basingstoke, Hampshire: Palgrave Macmillan, 2003), p83; Ronald Lewin, *Slim: The Standardbearer* (London: Leo Cooper, 1976), p140.

5   Michael Maccoby, "Narcissistic Leaders: The Incredible Pros, The Inevitable Cons", *Harvard Business Review*, (January-February 2000), pp68-77.

6   Jim Collins, "Level 5 Leadership: The Triumph of Humility and Fierce Resolve", *Harvard Business Review*, (January 2001), pp66-76.

7   Nigel Hamilton, *Monty: The Battles of Field Marshal Bernard Montgomery* (London: Hodder & Stoughton, 1994), p62, p68.

8   David French, *Raising Churchill's Army: The British Army and the War against Germany 1919-1945* (Oxford: Oxford University Press, 2000), p281.

9   Weinberg, *A World At Arms*, p444.

10 Montgomery was a Major-General commanding the 3rd Division under the II Corps of the British Expeditionary Force headed by then Lieutenant-General Brooke. See French, *Raising Churchill's Army*, pp178-179.

11 Slim commanded the 10th Indian Infantry Brigade in Eritrea where an inexperienced British Battalion broke and ran after coming under Italian air attack during the failed attempt to take the Italian fortress of Gallabat. See Robert Lyman, *Slim, Master of War: Burma and the Birth of Modern Warfare* (London: Constable & Robinson Ltd, 2004), pp4-5; Anderson, "Modern Manoeuvrist General", pp77- 78.

12 Slim, *Defeat into Victory*, pxiii.

13 Ibid., p121; Anderson, "Modern Manoeuvrist General", p79.

14 An example of many such episodes in the Burma Campaign took place during the desperate battle to extricate 1 Burma Division from Yenangyaung in April 1942. See Slim, *Defeat into Victory,* pp68-69; Lyman, *Slim*, p42.

15 For example, Slim took personal responsibility for misreading Japanese intentions during the run-up to the Imphal-Kohima battles in 1944 and failed to maintain a tight grip on his 4th Corps Commander, Lieutenant-General Geoffrey Scoones, by giving him too much leeway in deciding the timing of the withdrawal to draw in the Japanese units. See Slim, *Defeat into Victory*, pp294-295.

16 Ibid., p121.

17 Slim credited not himself, but the officers and men who served under his command for turning defeat into victory in Burma. See ibid., p551. This was not false modesty. Anderson noted that Slim deprecated narcissistic generals who ignored their soldiers' contributions to their success. One of Slim's soldiers, George MacDonald Fraser, would subsequently reminisce that when Slim spoke of what XIV Army had achieved, "it was always [in terms of] 'you' not even 'we' and never 'I'". See Anderson, "Modern Manoeuvrist General", p79. Fraser's observation was cited in Jon Latimer, *Burma: The Forgotten War* (London: John Murray, 2004), p417.

18 Slim, *Defeat into Victory*, p541.

19 Lieutenant-General Richard O'Connor's two divisions of 36,000 men routed the 100,000 men Italian 10th Army. See French, *Raising Churchill's Army*, pp212-213.

20 See Toh Boon Ho, "Book Review – Command or Control? Command, Training and Tactics in the British and German Armies, 1888-1918", *POINTER: Journal of the Singapore Armed Forces*, Vol.25 No.1 (January - March 1999), pp118-123.

21 Idem, "Book Review – Raising Churchill's Army: The British Army and the War against Germany 1919-1945", *POINTER: Journal of the Singapore Armed Forces*, Vol.28 No. 2 (2002), pp141-145; French, *Raising Churchill's Army*, p19, p45, pp55-57.

22 Stephen Ashley Hart, *Montgomery and "Colossal Cracks": The 21st Army Group in Northwest Europe, 1944-45* (Westport, Connecticut: Praeger, 2000), p164.

23 Weinberg, *A World At Arms*, p441; Hart, *Montgomery and "Colossal Cracks"*, p118.

24 In the process, Slim's XIV Army effectively destroyed the 150,000 men Japanese 15 Army, inflicting one of the Imperial Japanese Army's worst defeats second only to the Red Army's rout of the Kwantung Army in August 1945. See Weinberg, *A World At Arms*, pp641-642, pp858-860.

25 Slim, *Defeat into Victory*, p541.

26 Ibid., pp536-538.

27 Anderson, "Modern Manoeuvrist General", p82, p85.

28 For a good analysis of the transformation in the training of the Home Forces in the UK between1940-1944, see Tim Harrison-Place, *Military Training in the British Army 1940-1944: From Dunkirk to D-Day* (London: Frank Cass, 2000). For excellent studies on the transformation of the Indian Army following its defeat in 1942, see Daniel P. Marston, *Phoenix from the Ashes: The Indian Army in the Burma Campaign* (Westport, Connecticut: Praeger Publishers, 2003) and T.R. Moreman, *The Jungle, the Japanese and The British Commonwealth Armies at War, 1941-45: Fighting Methods, Doctrine and Training for Jungle Warfare* (London: Frank Cass, 2005).

29 French, *Raising Churchill's Army*, p280; Moreman, *The Jungle, the Japanese and The British Commonwealth Armies at War*, p102.

30 The two training divisions selected were the 14th Indian Division and the 39th Indian Light Division. See Moreman, *The Jungle, the Japanese and The British Commonwealth Armies at War*, pp91-97; Slim, *Defeat into Victory*, pp190-191.

31 In the interval period between 1939 and 1941, the Indian Army primarily trained for open warfare in the desert and not jungle training. The first official doctrinal pronouncement on jungle fighting was issued in 1940 by General Headquarters India as *Military Training Pamphlet No. 9 (India) Extensive Warfare: Notes on Forest Warfare*. In Malaya, Lieutenant-General Lionel Bond, General Officer Commanding (GOC) Malaya Command directed his General Staff Malaya Command to produce *Tactical Notes for Malaya 1940*. See Marston, *Phoenix from the Ashes*, pp42-43, p79; Moreman, *The Jungle, the Japanese and The British Commonwealth Armies at War*, pp12-24.

32 French, *Raising Churchill's Army*, pp204-206.

33 Slim, *Defeat into Victory*, pp188-189.

34 Hart, *Montgomery and* "Colossal Cracks", p100.

35 Slim, *Defeat into Victory*, pp161-162.

36 Moreman, *The Jungle, the Japanese and The British Commonwealth Armies at War*, pp84-86.

37 Following the disaster at First Arakan, General Giffard replaced Lieutenant-General Noel Irwin as GOC Eastern Army in May 1943. The creation of SEAC in August 1943 saw General Giffard become Commander-in-Chief, Land Forces and head of the 11th Army Group while Slim became Commander of the new XIV Army. See Slim, *Defeat into Victory*, p164, p168.

38 Slim, *Defeat into Victory*, pp186-187; Anderson, "Modern Manoeuvrist General", pp76-77.

LTA(NS) Toh Boon Ho is currently an Account Manager at International Enterprise Singapore. He obtained a BA (2nd Class Upper Honours) in History from the National University of Singapore in 1999 and a MSc (Strategic Studies) from the Institute of Defence and Strategic Studies, Nanyang Technological University in 2003. His current NS appointment is AG3, HQ Armour.

The Seven Technology Challenges for IKC2

by Mr Teo Chin Hock, Dr Yeoh Lean Weng, LTC Chew Lock Pin and Mr Teo Tiat Leng

Introduction

Integrated Knowledge-Based Command and Control (IKC2), the Singapore Armed Forces (SAF)'s version of Network-Centric Warfare (NCW), underpins the recent Revolution of Military Affairs (RMA) for the SAF. The SAF takes a very practical approach to network-centric warfare: IKC2 is about how we harness the power of the networks to win. This entails a mastery of sensors, shooters, communications, networks, information and command systems and orchestrating them to the best effect against the adversary.

It is often said that NCW is not about the technology but about people. This may be a truism but technologies must underlie this RMA. After all, where would e-commerce be without Internet technologies, or knowledge management without collaboration technologies? History tells us that the right technology will bring about sweeping changes to the way we do things. Hence, the key question is "which key technologies would dramatically change the way the SAF fights with IKC2?" In this article, we show how we can leverage the seven key technology areas, viz., networks, sensors, power, shooter, security, sensemaking, and collaboration to realize a quantum jump in operational capabilities.

Networks: Ubiquitous Connectivity

The fundamentals of IKC2 are network-centric and knowledge-based.[1] For the former, the goal is to provide soldiers with a ubiquitous information grid that he can tap into for information anytime, and anywhere, hence ubiquitous connectivity. Over the past few years, networks have proven to be catalysts for business revolution. We witnessed that as more network bandwidth becomes available, new ideas and applications rapidly emerged and consumed it. For networks, the question for the engineers is not "how much capacity should be built?", but "how to give the largest pipes to most people?"

People will use as much bandwidth as the infrastructure could provide. An interesting story in the SAF illustrates this. Two years ago, two command posts were wired up with 64 kbps of bandwidth. It was soon discovered that the line was completely blocked and nothing was getting through. As it turned out, a young and very IT-inspired officer had attempted to transmit an 18 MB Powerpoint file across the command posts. When advised that he should limit his file to 1 MB, he creatively broke up the 18 MB file into eighteen fragments, and sent out the 1 MB files individually! The network choked

on it and nothing was heard between the Command Posts thereafter. From this example and other experiences, we anticipate that our demand for bandwidth is directly proportional to the available bandwidth, with a proportionality constant always greater than "1".

Transmission technology, built around optical-electrical conversions, has given us the means to rapidly expand our bandwidth, doubling capacity 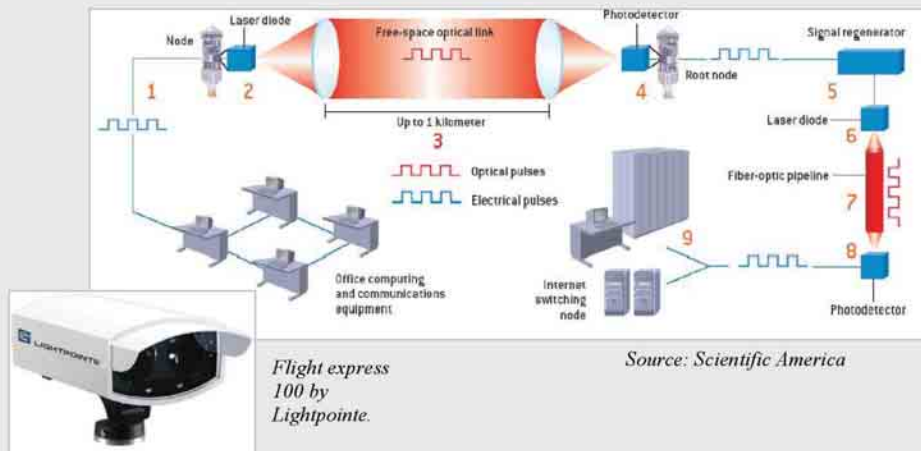every six months.[2] Are there limits to the expansion? Beyond exploiting Radio Frequency (RF) communications, high data-rate optical communications in the form of lasers (Free Space Optics) may further expand capacity because of its high frequency wave-form. Being less susceptible to detection by Electronic Warfare (EW) sensors, Free Space Optics (FSO) may permeate the last-mile tactical battlespace in the future. Today, a hybrid approach combining the reliability of RF, and the high data rate of laser communications is being developed by US AFRL, funded by DARPA[3] and is showing promise.

Free Space Optics

Free Space Optics (FSO) is "fiber optics communications without the fiber". The transmission medium used is low powered infra-red which offers 1 Gbps bandwidth. The key advantage of FSO is high bandwidth ranging from 10 Mbps to 1.25 Gbps, a goal beyond the reach of traditional Radio Frequency (RF) communications. Other key advantages include the ability to operate away from typical military communications frequencies, and hence avoiding governmental regulation, and high level of link transmission security due to very narrow transmitter beam width. At the same time, it has some serious disadvantages. As it rides on short wave lengths, it has limited range (up to 1km currently), requires line-of-sight and is prone to attenuation by environmental conditions such as clouds, foliage, sandstorms and fog. The best way to use FSO is for 'last mile' high-bandwidth connectivity, presupposing a high-bandwidth backbone (Satellites or Airborne Communications Node). FSO connectivity reliability within the local network could be enhanced by Meshed topology.

A project by AFRL and funded by DARPA, called the Optical and Radio Frequency Combined Link Experiment (ORCLE) program, is developing a hybrid solution of RF (reliability) and Laser (high bandwidth). The switching between transmission modes is adaptive and depends on the size of a message and on prevailing atmospheric conditions. So given a high content message, ORCLE will send it optically (high bandwidth), whilst the acknowledgement will be sent on the RF (high reliability).

FSO is already commercially available. US companies such as AirFiber and Lightpointe (picture shows commercially available LightExpress 1000) have FSO products.

Flight express 100 by Lightpointe.

Source: Scientific America

The drive towards rapid mobility, dispersion and on-the-move connectivity for maneuver forces adds to the challenge of "bandwidth never enough". Adm(Retd) Dennis Blair, in his speech "Full-Spectrum Transformation"[4], asserts that the modern battlefield is increasingly centered around the Edge (or frontline) units. In other words, local units need the most bandwidth. For peacekeeping and peace-making operations, edge units need the best information to make key decisions on the ground. Today's Combat Net Radios are reaching their limits in supporting such highly complex operations. To address bandwidth demand in built-up areas, there is an opportunity to exploit Commercial-Off-The-Shelf (COTS) wireless communications such as WiFi and WiMax to give us affordable bandwidth. Indeed, projecting to 2012, 4G networks could provide bandwidth of up to 100 Mbps globally and 1 Gbps locally.[5] Another key development is meshed networks whose architecture (sometimes described as 'spider-web' configuration) optimizes information throughput by making every node in the network a router, or an intelligent access point. For example, the Mobile Ad-hoc NETwork (MANET) was a DARPA funded project that enables mobility with meshed networks.

Sensors: Unblinking Eyes

With a reliable and robust network backbone in place, sensors sitting on this network will serve as our eyes and ears. The goal of the sensors is to "see first and see more" of the battlefield, a key tenet of IKC2.[6] The idea is to create a network of "unblinking eyes" that are enduring (persistence) and covers the entire area

of operations such that the adversary's movements could be detected and tracked. Therefore, the main challenges for sensing are persistence and coverage. Today, man-in-the-loop sensors such as airborne sensor platforms are limiting the proliferation of sensing over the area of operations because they are expensive. As unmanned technology becoming commonplace and highly affordable, the vision of unblinking eyes becomes realisable.

Norman Augustine[7] predicts, based on historical trends on the proportion of electronics as part of the aircraft's weight that there would be a point when the entire air platform is made up entirely of electronics! His illustration harbingers the day when the battlefield is largely surveyed and fought by machines and some autonomously. Today, a multitude of unmanned capabilities exists and are increasingly being exploited in innovative ways. Unmanned Aerial Vehicles were used extensively in Afghanistan, enabling small and dispersed forces the means to achieve information dominance over a far larger space than conventional forces could. Unmanned Ground Vehicle (UGV) has made early in-roads to deal with explosives detection and demolition, and may continue to see wider applications in counter-terrorism operations. Unmanned Underwater Vehicle (UUV) remains a player in surveillance missions (i.e. mine detection and sub-surface operations).
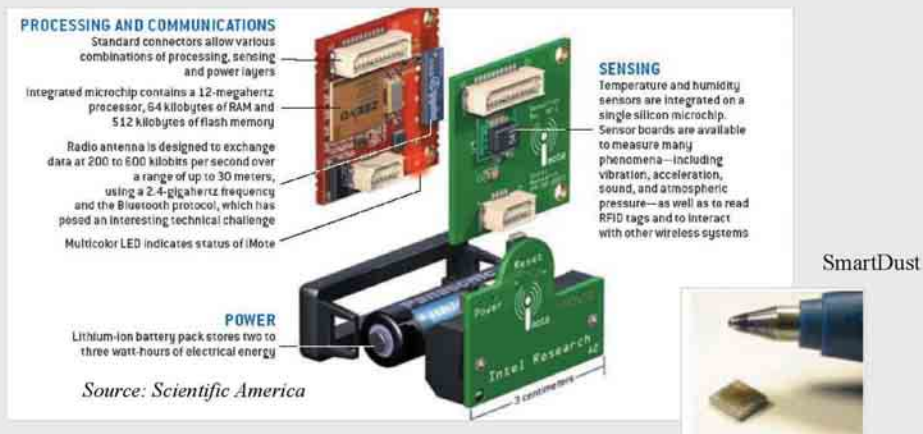
We are already exploiting unmanned sensors in our operations. For example, the Unmanned Surface Vehicles (USV) is now part of the force protection order of battle of the Republic of Singapore Navy (RSN), providing persistent presence

and extended reach whilst affording safety at stand-off distances. During the peacekeeping support operations in Iraq, the RSN deployed the Protector USV for surveillance operations in the Gulf.[8] The high-speed Protector, equipped with an electro-optic system, remote-control General Purpose Machine Gun (GPMG) and loud speaker, was used to establish and enforce protection zones around RSS Resolution and the Al-Basrah Oil Terminal. The Protector was deployed for prolonged operations, lasting up to eight hours per mission. Manned operations of a similar nature would have required a sizeable crew.

MOTES – "Macroscope"

Motes are thumb sized computers (memory capability). Attached with sensors, transceivers and wireless communications, they could form a smart, autonomous, sensing network with other similar nodes. Think of these as mini PCs. They are cheap enough to be deployed in thousands and across a wide area. Collectively, the network of Motes forms a Perceptive Network or "Macroscope", to pick up data over a large area, so that trends and interdependencies across the area could be detected. This technology was academically and commercially motivated and used by biologists to study animal behaviors in an ecosystem, and by manufacturing plants to monitor critical machinery. To enable these "PCs" to function, "lightweight" operating systems and applications were developed. The TinyOS is an operating system designed for the motes and is extremely stingy with energy. The TinyDB is a distributed database of the motes and it enables queries to be made across the nodes all at once. These software were developed by teams from Berkeley and Intel. The smallest mote today is the SmartDust, developed by Berkeley. It is a 5 square millimeter device with the TinyOS functions weaved into the hardware in order to reduce footprint. Energy to power the SmartDust is harvested from ambient light or vibration. By dispersing SmartDust over the Area of Operations (AO), a military force could potentially sense and map the "global" movement of enemy forces, rather than capturing piecemeal pictures by today's sensors, which has limited loiter time around each segment of the AO. Commercial versions of Motes are available and they are manufactured by US companies Intel and Crossbow.

PROCESSING AND COMMUNICATIONS
Standard connectors allow various combinations of processing, sensing and power layers

Integrated microchip contains a 12-megahertz processor, 64 kilobytes of RAM and 512 kilobytes of flash memory

Radio antenna is designed to exchange data at 200 to 600 kilobits per second over a range of up to 30 meters, using a 2.4-gigahertz frequency and the Bluetooth protocol, which has posed an interesting technical challenge

Multicolor LED indicates status of iMote

SENSING
Temperature and humidity sensors are integrated on a single silicon microchip. Sensor boards are available to measure many phenomena—including vibration, acceleration, sound, and atmospheric pressure—as well as to read RFID tags and to interact with other wireless systems

POWER
Lithium-ion battery pack stores two to three watt-hours of electrical energy

SmartDust

Source: Scientific America

Unmanned Ground Sensors (UGS) is a new class of low cost, pervasive, and wide-coverage sensors. Scattered across a wide area, they could collectively form a 'Macroscope', or a perceptive network that presents not just the local picture around each sensor node but interdependencies and trends across the entire area. Today, commercial versions, popularly known as Motes, are being used for various purposes such as monitoring critical machinery in manufacturing plants or to help scientists monitor climates or ecological environments.[9] These could be adapted for battlefield deployment disguised as natural objects, such as rocks.[10] Over time, with the commercial push and the advancements of technology, it will become affordable to deploy widely in the battlefield[11], providing us with the persistence and comprehensive coverage in sensing.

Shooters: Many and Cheap

The Gulf Wars have demonstrated how shooters have become more precise over the years. Beyond precision, NCW will add a new dimension to the notion of shooting. Given a network of shooters, there is now the opportunity to coordinate and mass multiple shooters to produce not just precise shooting, but precise effects; networked shooting could precisely calibrate the outcome (e.g. extent of destruction) not just over one target but over an influence network of interdependent targets. With a variety of shooters having various degrees of accuracy and sophistication, and an effective network to orchestrate them, effects-focused and cost-effective shooting can be achieved.

Cost effectiveness is becoming an important factor for shooting, because target varieties are increasing and are becoming cheaper. Barnett in his seminal discourse on the *Seven Deadly Sins of Network-Centric Warfare*[12] spoke about Avarice and the economics of NCW, and asserts that NCW favors the "many and cheap". When we reason about the economics of shooting, we have questions such as "is it sustainable to invest in sophisticated but expensive missiles when targets (such as UAVs) are getting cheaper?" Indeed, we see a proliferation of cheap and innovative ideas that could achieve cost-effective shots by putting new gadgets over outdated munitions. For example, the war-tested JDAMs (Joint Direct Attack Munitions) reuses the warhead and fuse of the Vietnam-era iron bombs, but made precise with advanced GPS-guided Inertial Navigation System (INS) add-on kits for guidance; and the US Army Advanced Precision Kill Weapon System (APKWS) reuses the rocket motor, launcher, warhead and fuse of their existing Hydra-70 Rocket System, and made precise with a new laser sensor and guidance package, they are capable of precision of one metre. As a result the JDAM costs US$14K and the APKWS costs US$10K per shot. The motivation for the APKWS stemmed from the need to have a cheaper option to take out cheaper targets. The operational experience of Desert Storm was that many expensive HELLFIRE missiles, designed for anti-tank purposes, had to be used against non-tank point targets.[13]

Another key development is directed energy weapons.[14] Aside from other important advantages of using lasers such as precision and 'masslessness' (i.e. negligible influence by gravity), cost may be the factor that ultimately makes lasers most compelling. The US Army was running the Tactical High Energy Laser (THEL) programme to develop a viable Anti-Missile laser system that has the potential to deliver both precision and cost effectiveness.[15] When THEL was found to be too bulky, the Mobile-THEL follow-on programme was initiated. With M-THEL, the cost of a single shot could cost US$8K instead of US$3.8M. The system would also become a more suitable weapon against typical threats such as mortars and rockets. The sci-fi future of 'Star Wars' may not be too far off.

Power: Always On

Ubiquitous networks, persistent sensing or mass, directed-energy shooting cannot function without reliable power sources. Power sources must improve in persistence and reduce in size to support the net-centric paradigm. As described above, sensors could be miniaturised to the size of a pebble, even to a peck of dust. Similarly, power sources must also shrink and be able to provide long-lasting power to sustain prolonged operation of the sensors, shooters and networks, some of which would be autonomous. A
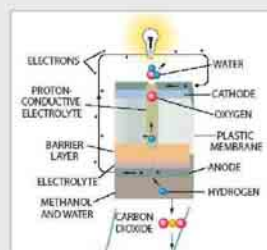
power management strategy needs to be developed to manage the diverse power requirements of a varied operational environment as defined by IKC2.

Alternative power sources such as hydrogen fuel cell, solar power, and kinetic-power would extend the typical sustainability and portability of power supplies today. Fuel cells are gaining in promise because of its higher storage of electrochemical energy (translating to long hours of operation) and its amenability to miniaturization. In 2005, a company called Millennium Cell demonstrated its prototype fuel cell based on hydrogen fuel cell technology that was able to power an IBM ThinkPad several times longer than conventional batteries.[16] Another report by ZDNet[17] suggests that production models of a fuel cell prototype will be commercially available in 2007, providing fourteen hours of laptop power. The next challenge is to make fuel cells compact enough for portability and sustainability for field operations. This is not trivial because the problems of over-heating need to be managed.

Fuel Cell Technology

Fuel cells can liberate significantly more electricity from chemicals such as methanol and similar hydrogen based fuels compared with traditional nickel-cadmium batteries (See table below). Most fuel cell research has focused on developing the alternative for automotive fuel. Car makers such as Toyota are already test-running versions of Fuel Cell Hybrid Vehicle (FCHV) using pure hydrogen or methanol. Meanwhile, there are efforts to miniaturise fuel cells to provide power to a wide range of day-to-day gadgets such as mobile phones and laptops. If successful, the potential is to have mobiles run for weeks and laptops run for hundreds of hours without the need to recharge batteries. Challenges to overcome for miniaturisation are: management of hydrogen-based fuel and problems of over-heating.

THE ENERGETIC POTENTIAL OF FUEL CELLS

	STORED ELECTROCHEMICAL ENERGY (in watt-hours)	
	By mass (per kilogram)	By volume (per liter)
FUEL CELLS		
Decalin ($C_{10}H_{18}$)	2,400	2,100
Liquid hydrogen	33,000	2,500
Lithium borohydride ($LiBH_4$ and $4H_2O$)	2,800	2,500
Solid metal hydride ($LaNi_5H_6$)	370	3,300
Methanol	6,200	4,900
Hydrogen in graphite nanofibers	~16,000	~32,000
RECHARGEABLE BATTERIES		
Lead acid	30	80
Nickel-cadmium	40	130
Nickel-metal hydride	60	200
Lithium-ion	130	300

Source: Scientific America

Fuel cells whilst lasting longer still require replenishment. This leads to demands for support in the form of spare batteries and generators that would add to the inventory of a logistics train. Innovation in the area of power supply for mobility must be made. Kinetic (motion and wind) and solar power "makes" energy from the natural resources of the operating environment and could be self-sustainable. Today, foldable and lightweight portable solar panels exist[18], but the size remains a challenge for many applications.

With a combination of power sources, and longer running hours, global power resource planning should be carried out to exploit the combination of stored (batteries or generators) and natural energy sources such as wind, kinetics, and solar energy to the fullest. This may lead to future Command Posts and nodes being self-sufficient in power; to the extent that it would not need to be accompanied by cumbersome generators and power cables. In this way, the future Command Posts can be very small, covert, and highly mobile.

Sensemaking: Cognitive Edge

With IKC2, the commander may become the "weakest link" in the system of systems. Due to the increased number of sensors and network coverage, he would be flooded with information that may be too much for his limited cognitive capacity to handle. Rather than achieving information dominance, the commander may find himself overwhelmed by information. Today, computing is providing us with a whole new set of opportunities to alleviate the cognitive limitations of

humans and at the same time amplify his cognitive strengths. The Future Systems Directorate (FSD) of the SAF has articulated that sensemaking capability is to *create the cognitive edge*[19] for the 3rd Generation SAF. The cognitive edge describes a state of superiority in cognition, articulating the SAF's ability to become more adaptive, mentally prepared, cognitively sharper and faster, and working more coherently as an organisation.

The Internet revolution is bringing about a myriad of technologies that aims to help people deal with information – searching (finding the needle in the haystack), managing, aggregating, summarising, and creating knowledge, to name a few. The Google phenomena, with highly popular applications such as the famous Google search engine and the Google Earth[20] applications, are examples of tools that help us get to information quicker. The sensemaking capability is about information search and more. In order to truly help the commander find and make sense of information, we need a good understanding of the cognitive psychological profile of the commander and how to best utilise technology and techniques to support his cognition. Information (or Sensemaking) Technologies must be built around the cognition of the human. Technologies, such as visualisation, will help the commander's cognition by helping him externalize his working memory and enhance his generation of pattern recognition for improved intuition. Another important effort, of which DARPA is major sponsor, is the Augmented Cognition programme. The idea of Automated Cognition is to tap the cognitive states of people using neuro

and psycho-physiological measurement devices, and to use these data to feedback to the computing system, which than autonomously optimises computing resources to tailor the information ingestion rate. This is a first step towards creating a computer that is symbiotic with the human.
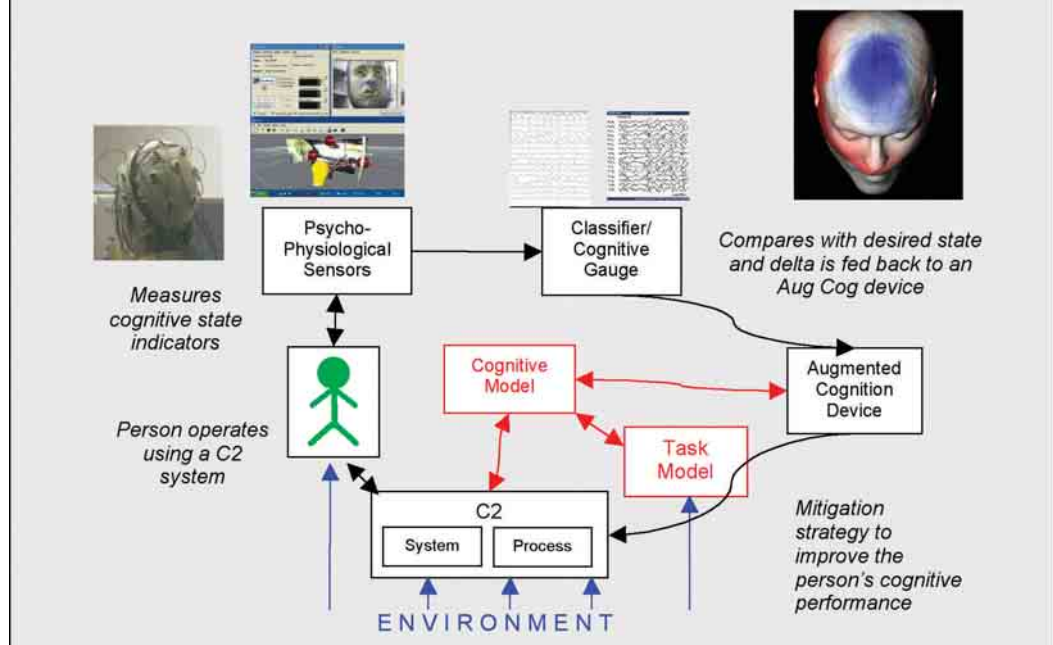
An important sensemaking effort in Singapore is the project called Risk Assessment and Horizon Scanning (RAHS) System, championed by the National Security Coordination Centre (NSCC).[21] Working with Dave Snowden and futurist John Peterson of The Arlington Institute, RAHS aims to ingest data from a multitude of information sources - including open source information from the World Wide Web - and seek to help analysts detect weak signals buried in noise. Embedded in the codes are ideas founded on a sound understanding of human cognition, e.g. 'suspending belief' is the notion of not mentally committing to a mental model (a typical human bias), but to stay cognitively agile and sensitive to unconventional possibilities, a key to weak-signals detection. Technology exists today to enable us to manage complexity, to

Augmented Cognition

Augmenting cognition is about using state-of-the-art computing to complement human and team cognition. When achieved, we anticipate a state of human (or team) and computer symbiosis. DARPA's programme for example, focuses augmentation on increasing information intake under stress or high workload. It aims to achieve an order of magnitude improvement in performance through adaptation strategies that mitigate against the detrimental effects of workload. In addition to mitigating weaknesses, augmented cognition has the potential to also amplify cognitive strengths.

The diagram shows an example of how an Augmented Cognition system might work. Psycho-Physiological Sensors (e.g. EEG) can be used to capture the cognitive state (blood flow or electrical activations in the brain) of the person. The state is then measured against a desired state and fed back to a device, the latter designed with a context dependent cognitive model. The device will drive changes to the C2 system processes that would attempt to manage information throughput to a level commensurate with the person's desired cognitive state.

mine and extract the relevant information and weak signals, and to help the analysts connect the relevant dots. It would enable us to enlarge our understanding of the current situation and expand the envelope of possible futures.

Collaboration: Connected Minds

"Humans are born collaborators. We are social animals and almost every worthwhile development or achievement is the result of group effort... Trust has always been a key issue intertwined with collaboration."

- Kruse & Adkins[22]

Many would conclude that IKC2 is simply about networking the systems, such as the sensors and weapons we have covered earlier. On top of that, a key outcome of IKC2 should be better command and control. Increased knowledge sharing should result in better decision-making and orchestration of multiple actions to produce better and precise effects. All these are the results of connected minds.

Better synergy in purpose does not just happen. A set of technologies is needed to foster it. The web provides illuminating examples of how people have found ways to work together.

Mash-Up Technology

A **mash-up** is a website or web application that seamlessly combines content from other sources into an integrated experience and all these can be done voluntarily by people over on the Web. This capability is enabled by the 2nd generation of Web Technology - Web 2.0, which enables people to build interactive desktop web applications, rather than the traditional static web pages. The technology makes available simple and lightweight API's (Application Program Interface) that are easy to design and deploy. In this way, unlikely innovators were lured to put forward their data and combine different data sources in new ways. Examples of interesting Mash-ups are the Chicago Crime (http://www.chicagocrime.org), web site of the birthplace of Oscar winners (http://www.mibazaar.com/oscars/index.html), and WeatherMole (http://weathermole.com/WeatherMole/index.html). WeatherMole is a collaboration of the National Centre for Atmospheric Research (NCAR), Google Map and Google Suggest. WeatherMole came to be because a software engineer of NCAR thought it would be a good idea to integrate the weather forecast application from National Oceanic and Atmospheric Administration's (NOAA) Experimental National Digital Forecast database XML Web Service to Google Maps. An interesting blog to browse is one dedicated to Google Mash-ups (http://googlemapsmania.blogspot.com/). People are creating new knowledge on-the-fly.

The WeatherMole showing the weather of a location in US for the next 5 days.

Beyond the ubiquitous electronic-mail, instant messaging, chats and video conferencing, netizens have introduced the Wikipedia, Mash-up technologies, Grid computing, and the Open Source movement. All these, enabled by web technologies have produced outcomes in the form of the Wikipedia encyclopedia (over a million entries currently), the SETI@ home project, Google Earth and the Open Office suite that are all free, but highly sophisticated products. It shows how ingenuity emerges when you create technologies that enable people to collaborate.

What do such collaboration technologies mean to IKC2 for the SAF? If the technological means mentioned above is offered to SAF soldiers and planners, and given the new generation's increased competency with technology, new creative ways of knowledge sharing and generation would be fostered. A new generation of network warriors would emerge. These are warriors who know the ins-and-

Artificial Immune Systems (AIS)

The AIS effort is a variant of the multi-agent system effort. The approach is to use Human Immune Systems (HIS) principles and characteristics to build systems that could configure, learn and adapt to new environment conditions autonomously. A key effort of AIS is to deal with System Assurance issues, i.e. to deal with system breakdowns and malicious virus attack. To illustrate the effort, we refer to a development by a Swiss research institute, called the Laboratory for Computer Communications and Applications. The effort by the Institute is to detect Routing Misbehaviours in Dynamic Source Routing (DSR) in mobile ad hoc networks (see figure). The architecture is a "protect dynamic-self" approach – each node in the network is protected by an AIS node that forms a network with other AIS nodes (a meta-network; the architecture is similar to IBM's Autonomic Computing). This system aims to be able to automatically learn and detect new misbehaviour, but at the same time remain tolerant to previously normal behaviour. The challenge of the system is to be sensitive to false positives. The 4 main blocks are HIS based – Danger Signal; Virtual Thymus; Clustering and Clonal Selection. How does it work? The AIS system watches for DSR protocol events. When there is a Danger Signal (DS) such as an event of Packet Loss, a signal is sent to 3 places: the Virtual Thymus, Clustering and Clonal Selection modules. The Thymus generates 'antibodies' (patterns of protocols) to match the Danger Signals. The 'antibodies' are generated from the 'Bone Marrow' module, which has a repertoire of protocol patterns captured (learned) offline via simulation. Like the biological parallel, either a match is found or a process of cloning of antibodies (variants) is started to create a diverse set of antibodies to find a better match for the DS at the Clonal Selection Module. The matches are further clustered at the 'Clustering' module so as to capture the high rates of matches as a process to reduce the incidence of false positives.
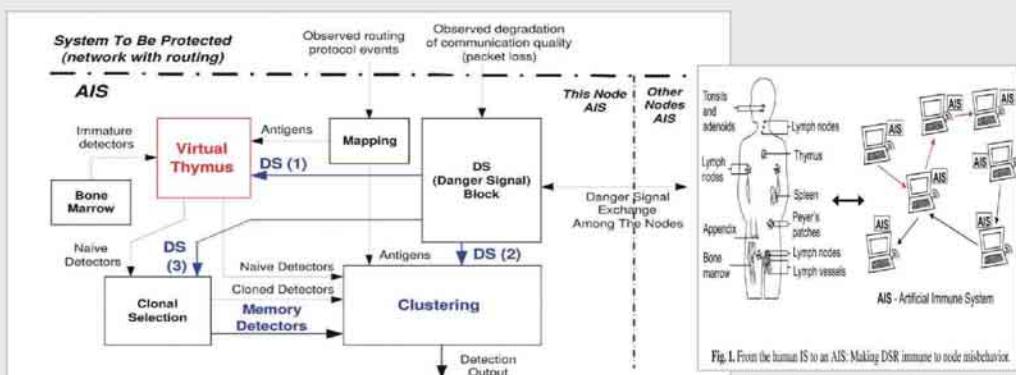

Fig. 2. AIS building blocks in one network node. *Note:* DS(1), DS(2) and DS(3) are all the same danger signal, indexing only emphasizes three different uses of it.

Fig. 1. From the human IS to an AIS: Making DSR immune to node misbehavior.

Human Immune System (HIS)

Artificial Immune System

outs of the invisible network grid, and are able to exploit it fully to synchronise their actions with other partner warriors to fulfill their goals.

Security – Immune Networks

As the SAF exploits infocomm technology to achieve IKC2 network-centricity to bring about that quantum jump in operational effectiveness, it will also become more dependent on the network. Being dependent on the network would allow adversaries to exploit this vulnerability and wage cyber-war on the net to cripple operations that depend on it. Therefore, network security is the last but certainly not the least of the key challenges. If information received from the network, say GPS information for targeting is adulterated and becomes unreliable, then confidence with the IKC2 capability will be affected.

However, in considering net security, a dilemma surfaces - security limits the freedom of exploitation of information, the very thing it is trying to preserve and liberate. The challenge is to find the right balance between imposing robust security (fortress) versus allowing freedom of information exploitation. It is difficult to establish "What is enough security?". We believe the answer is "It depends" on the context or scenario. Hence, a viable security structure must be similar to the human immune system where it has a repertoire of mechanisms to tackle typical attacks, but at the same time has self-learning and adaptive mechanisms that apply new strategies to tackle new types of attacks. The idea for security is not to build a fortress, because it is too costly and likely to limit flexibility, but to build an adaptive network with sensors sensitive to the viral environment and with mechanisms that learn and build new response mechanisms. There are new trends in this direction. Hewlett Packard's (HP) Virus Throttle software does not take the traditional scanning solution based on known viruses but instead monitors for abnormal, virus-like behaviors. Once such behaviors are detected, the system will gradually slow down the connections with the possible infected machines so that the administrator could take remedial action.

A more ambitious approach is IBM's Autonomic Computing which aims to create a framework of computing with self-healing and self-protection built-in. Another thrust is in the more academic area called Artificial Immune System, which develops agent-based solutions that parallels biological immune systems.

Conclusion

This paper has surfaced seven technological challenges for IKC2. Whilst they are challenges, they are also opportunities. When these challenges are overcome, immense opportunities become available to dramatically change the way we fight. These seven technology areas would underlie the SAF's RMA in IKC2. However, new operational concepts cannot materialise without the ingenuity of people; the technologies offer a foundation where many new possibilities arise, but it is up to the ingenuity of people to innovate with them to create viable solutions to solve operational problems. The SAF must tap the technology savvy generation of young operators and technologists to invent and break new ground in both concepts and technology. The ability to harness the

asymmetry of such technologies may well determine the winners and the losers of future conflicts. ⊚

Endnotes

1 Jacqueline Lee et al. "Realising Knowledge-based Command and Control". POINTER Monograph No. 2. http://www.mindef.gov.sg/imindef/publications/pointer/monographs/mono03.html. Mar 2003.

2 Jim Pinto, "The 3 Technology Laws". http://www.jimpinto.com/writings/techlaws.html. Last accessed: 30 Oct 2005.

3 Henry Kenyon, "Light and Radio Harmonized on One Channel". AFCEA Signal Magazine. http://www.afcea.org/signal/articles/anmviewer.asp?a=505. Nov 2004.

4 Adm(Retd) Dennis Blair, "Full Spectrum Transformation". Institute of Defense Analysis. 12 Sep 2005.

5 Anders Lotsson, "Expect 4G Telephony in 2012". Computer Sweden. 10 May 2004.

6 Jacqueline Lee et al. "Realising Knowledge-based Command and Control". POINTER Monograph No. 2, pp 14, http://www.mindef.gov.sg/imindef/publications/pointer/monographs/mono03.html. Mar 2003.

7 Norman Augustine, "Augustine's Laws". Penguin Books, p96. 1986. Norm Augustine became famous with his prediction by his Augustine's Law XVI, which predicts that by 2054 even the US would not be able to afford a single tactical aircraft. Augustine's Law XIV states: "After the year 2015, there will be no airplane crashes. There will be no takeoffs either, because electronics will occupy 100 percent of every airplane's weight."

8 Cheng Kiat Loon, "The Next Wave". Cyberpioneer. http://www.mindef.gov.sg/imindef/publications/cyberpioneer/features/2005/may05_cs.html. 15 May 2005.

9 D. Culler, and H. Mulder, "Smart Sensors to Network the World". *Scientific America*, 2004.

10 Reuters, "Russia Claims Rock-solid Evidence of British Spying". Article in The Straits Times newspapers reporting on the discovery of an electronic communication device hidden as a rock found in the outskirts of Moscow. 24 Jan 2006.

11 Chris Broz, "Stealthy Observer". C4ISR magazine Vol 4, No. 6 Jul 2005.

12 Thomas Barnett, "The Seven Deadly Sins of Network-Centric Warfare", US Naval Institute, http://www.nwc.navy.mil/WARDEPT/7deadl~1.htm. 1999.

13 http://www.globalsecurity.org/military/systems/munitions/apkws.htm

14 Jonathon Skillings, "Are Laser Weapons Ready for Duty?" C-Net News.com article. http://news.com.com/2008-1008_3-6059967.html. Last accessed: 17 Apr 2006.

15 The Mobile-THEL programme followed the THEL programme to give mobility to the laser.

16 Shirley Georgi, "CES - Baubles, Bangles and Batteries". Article on Batteries Digest website, reporting on the 2005 Consumer Electronics Show. http://www.batteriesdigest.com/id430.htm. Last accessed: 4 Feb 2006.

17 Stephen Shankland, "Fuel Cell Offers 14 Hours of Laptop Power". ZDNet news report on emerging fuel cell technology. http://news.zdnet.com/2100-1040_22-6047966.html. 9 Mar 2006.

18 RadioLabs website. "Solar Panels". Website brochures marketing rugged solar panel products. http://www.radiolabs.com/products/electronics/power/solar-panel.php. Last accessed: 5 Oct 2005.

19 Future System Directorate Sensemaking Framework coined the notion the cognitive edge. The Cognitive edge is defined as the ability to make faster and better decisions than the adversary. The operational manifestation of the cognitive edge is Cognitive Asymmetry, which can manifest as having an overwhelming cognitive superiority over the adversary, or being able to match large amount of cognitive activity within the adversary's organisation with a relatively smaller amount of cognitive resources.

20 Google, "Google Earth Home" website. http://earth.google.com/. Last accessed: 30 Oct 2005.

21 Farah Abdul Rahim, "Singapore to Develop Terror Risk Assessment and Scanning System". Channel News Asia article. http://www.channelnewsasia.com/stories/singaporelocalnews/view/175366/1/.html. 26 Oct 2005.

22 John Kruse, and Mark Adkins, "The Technology Trap". Aug 05 issue of the *Proceedings* magazine of the US Naval Institute (http://www.navalinstitute.org), Aug 2005.

Mr Teo Chin Hock is currently DSTA Director (Networked Systems). He has more than 20 years of experience in the C4I domain. Mr Teo had served as an Air Engineering Officer in the RSAF. He was subsequently involved in the acquisition and development of C4I systems in air defence for the RSAF, and led in the development of several shipborne C4I systems for the RSN. Since the inception of DSTA, he joined the organisation as a Director to oversee the development of C4I systems and solutions for the Singapore Armed Forces and other national security agencies. He holds a Bachelor of Engineering (1st Class Honours) and a Master of Science (Electrical Engineering) from the National University of Singapore, and a Master of Science (Electrical Engineering) with Distinction from the US Naval Postgraduate School.

Dr Yeoh Lean Weng is Acting Director (C4I Development) at DSTA. He is also concurrently, Deputy Director of TDSI at NUS. He received his Bachelor (with Honours) and Master of Science degrees from NUS in 1983 and 1987 respectively. He further obtained two Masters (Distinction) in 1990 and a PhD in Electrical Engineering in 1997 from the Naval Postgraduate School (NPS). He attended the Programme for Management Development from Harvard University in 2003. He received the National Day Public Administration Medal (Bronze) in 2001, and the Defence Technology Prize in 1992 and 2004. He has extensive experience in the development and implementation of Command, Control Communications, Computers and Intelligence (C4I) systems.

LTC Chew Lock Pin, a Naval Warfare Officer by training, is currently an Assistant Director at Defence Science and Technology Agency and concurrently an Assistant Director at Future Systems Directorate. LTC Chew has previously commanded a Missile Gun Boat and have served onboard the Missile Corvettes. He holds a Bachelor of Science (1st Class Honours) in Physics from Imperial College, University of London, U.K., and a Master of Technology in Knowledge Engineering from the National University of Singapore. He was a recipient of the Defence Technology Prize in 2005.

Mr Teo Tiat Leng is currently Assistant Director (C4I Development) at DSTA. He has 15 years of experience in the development of C4I systems for Joint and the Army. He holds a Bachelor of Science (Computer and Information Science), a Master in Defence Technology & Systems and a Master of Technology (Software Engineering) from the National University of Singapore, and a Master of Science (Computer Science) with Distinction from the US Naval Postgraduate School.

SAFETY – Keeping Abreast with Transformational Efforts

With reference to MAJ Tay Gek Peng's article "The Human Perspective of Safety – A Flight Commander's Reflection" that was featured in the last issue, I agree with his view that Leadership is "a cornerstone to building and sustaining an effective safety culture". This translates to the fact that safety must primarily be "top-down" driven. However, Leadership cannot act alone without having the people onboard. As a result, there is this need to have a shared value like Safety. In the RSAF, Safety is indeed a core value, and is central to our training and operations. The writer's proposed "human level strategies", to rejuvenate the safety movement within the RSAF, is refreshing. It espouses the value of the individual's contribution to the overall safety movement and it promotes innovation through safety.

The proposed strategies by the author complement the RSAF's four safety principles, which form the core of the RSAF's deeply entrenched safety culture and encapsulate the RSAF's fundamental beliefs on accident prevention. However, *an increased operational tempo post-911 coupled with transformational efforts towards a 3rd Generation RSAF formed an impetus to review our principles of safety*. This resulted in a refined RSAF fourth safety principle that was rolled out in Oct 05. Let me elaborate on it.

The New Operational Paradigm

In recent years, the operational tempo has increased substantially with high-end training for conventional warfare, sustained vigilance and OOTW missions being conducted concurrently. While the RSAF has developed the agility to quickly switch between the different operating modes, *commanders and airmen are constantly being challenged to strike the balance between achieving mission results and managing the risk level for overall mission success.* The

operational environment of the future will be increasingly complex, dynamic and uncertain, characterised by cutting-edge technologies, new concepts and organisational restructuring. Our people must be able to simultaneously discern the different demands made on safety and across the wide spectrum, ranging from conventional operations, to increased experimentation, to the realm of training for uncertainty. Logistically, we will also see a shift towards a more NSmen/NSF-centric, multi-skilled, multi-disciplined technical workforce, as well as commercialised support becoming more prevalent. *Significantly, this time, we are at the frontiers and our airmen will be faced with challenges in various areas, with no precedence to fall back upon.*

Safety – A critical responsibility

The strategy for the RSAF is to continue to build upon the strong safety culture inculcated over the years, with the following key thrusts and initiatives at the individual, team and commander level:

• *Safety as an individual's responsibility* as the 3rd Generation transformational effort will see greater decision making down to the individual level where dynamism and uncertainty prevails. The solution is through the process of *internalising safety*, making it one of the personal beliefs. Individuals, then, in essence move away from processes, to the ability to think from "first principles" on how to balance operations with safety.

• *Safety as the team's responsibility* as a network centric operation requires that safety from the various components complement each other through effective integration. Team safety works through the use of Threat and Error Management CRM (TEM-CRM), where both *operational and safety task loading are shared among members of the same team, and at all levels of the organisation*. Behavioural Based Safety (BBS) initiatives used to identify specific behaviours also depend on team excellence to maintain a safe working environment.

• *Safety as the commander's responsibility* as the emphasis in safety must continue to be top-down, with commanders giving the appropriate emphasis. The "Zero Accident" goal can then be realised through strong visioning and sound guidance. Moreover, *the commander's belief in its possibility is pervasive across all ranks, thus ensuring safe practices at all levels.*

The old 4th RSAF Safety Principle having "Safety is a command responsibility that requires the participation of everyone" was thus replaced with the new principle that reads as "Safety is an individual, team and command responsibility".
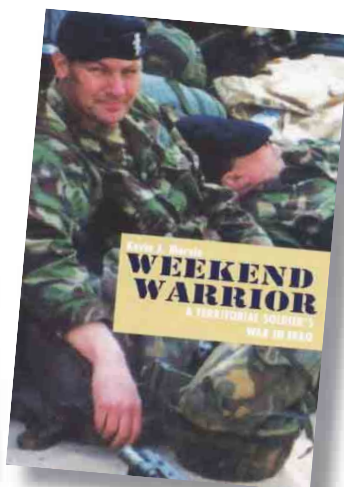
This change, amongst others, was necessary to better reflect the shared responsibility now taken across the entire spectrum of our organisation, especially against the backdrop of dynamism and mission uncertainty. In our endeavour to transform our organisation into a modern fighting force, safety must move in tandem with renewed strength and spirit to meet the challenges of increased operational complexity.

COL Kevin Teoh
(Head, Air Force Inspectorate)

Out of Evil

by Mr Toh Ee Loong

Stephen Chan, *Out of Evil: New International Politics and Old Doctrines of War*
(London: I.B. Tauris, 2005).

Kevin J. Mervin, *Weekend Warrior: A Territorial Soldier's War in Iraq*
(Edinburgh: Main Stream Publishing, 2005).

"**O**ut of evil can come great good", said US President George W. Bush shortly after the events of September 11. Mr Bush went on to describe the threat of an Axis of Evil during his State of the Union address on 1 September 2002. Prof Stephen Chan examines how the War on Terror became a War on Evil and argues that the language of good and evil is of limited use in the pursuit of national security. Conversely, the unlimited demands of such logic can be hugely counter-productive. Besides his academic background as Professor of International Relations in the University of London and foundation Dean of Law and Social Sciences at the School of Oriental and African Studies, Prof Chan also draws on his varied experiences as a poet, international civil service with the Commonwealth Secretariat and national karate coach of Zambia to write a book aimed at the layman.

Complementing his scholarly, philosophical and literary sources, the author uses prominent events reported by the media and popular culture such as the destruction of the rock-cut Buddhas at Bamiya by the Taliban or

the movie *Independence Day* to give brisk yet nuanced accounts of how the regimes of the Axis of Evil came to be. Thus Prof Chan also attempts to remedy the shallow understanding of broader historical context underlying the politics of Afghanistan, Iraq, Iran and North Korea. Great care is taken not to excuse or romanticize the character of these states or their rulers. But these histories, as opposed to a reductionist narrative of good versus evil, are meant to demonstrate that however eccentric, inscrutable or dangerous these states may seem, they should not be reduced to being "evil" as they are still essentially rational actors – the conduct of relations with such states has to appreciate that their *raison d'etat* is bounded by their own idiosyncratic circumstances.

The most thought-provoking and relevant portion of the book for readers of *POINTER* is Prof Chan's diagnosis of the US leadership's attempt to vanquish evil with new technology and military power. Cued by the subtitle of "new international politics and old doctrines of war", the book argues that the US is still fighting in the way that it planned for in the Cold War era. The policy direction of the US administration and the strategic logic of the Pentagon's military planners is still essentially state-based. The author sees the concentration of US effort against the conveniently state-delineated enemies of the Taliban in Afghanistan and Saddam Hussein in Iraq as evidence of how the US's strategic imagination is still delimited by borders, its objectives continued to be rooted in a desire to seek a Clausewitzean annihilatory and decisive victory against standing armies and platforms in spite of a threat that is much more diffused and nebulous.

The book does not draw on or engage with the US military's burgeoning literature on force transformation expressed in the 2001 and 2006 Quardrennial Defence Review (QDR) reports and the 2005 National Defense Strategy document. These show strong cognizance of how the US military needs to adjust to cope with threats arising from "dispersed non-state networks" and shift from a threat-based to an effects-based doctrine. However a closer reading of how these official pronouncements will be implemented show strong continuity rather than radical change. The International Institute of Strategic Studies' *The Military Balance 2006* opines that the 2006 QDR "made little alteration to the long list of equipment programmes currently under development" and pointed out that although it outlined plans for transformational investment, no corresponding cuts were made in traditional areas of spending, "suggesting that difficult budget decisions… have yet to be made".

Events post-publication have lent further credence to Prof Chan's assessment that US grand strategy continues to rely on its technological superiority to deliver meaningful victory – in effect, hope is now a strategy. However, in the past months, outbursts of frustration from eight retired senior generals underline how, despite deploying the best technology and "transformed" military that induces "shock and awe", the US military looks more like it is being dominated by the full spectrum's lower end rather than the other way round.

In contrast to Prof Chan's book, Lance Corporal Kevin J. Mervin's autobiographical account of his experiences in Op Telic, the British code-name for the war in Iraq, is a view so close to the ground that you can almost hear the constant rumble of military vehicles and feel the desert heat. When narrating in the first person, some passages are replete with expletives and military jargon – with a twelve page appendix and glossary dedicated to explaining the latter.

The book has several strengths that make it both an insightful and entertaining read. Mr Mervin gives a voice to unglamorous segments of the military that many civilians may be unaware of and even those within the military take for granted. His good humour and lack of hesitation to relate problems of his own making make his story easy to digest. He served as a member of the UK Territorial Army (TA) – somewhat like the US National Guardsman. Another distinguishing feature of Mr Mervin's point of view is that of his vocation. He belonged to the logistics family as a heavy vehicle recovery mechanic. Throughout the book, he encounters and counters prejudice against the TA from regulars who deride the TA as "weekend warriors". Mr Mervin's fierce pride in the TA can be traced to the confidence stemming from serious military and vocational training which is enhanced by complementary civilian skills and experience. The opening and closing chapters which vividly describe his personal reaction, as well as those of his family, to his call up and subsequent return successfully convey the anxiety of the transitions from civvy street to war zone and back.

The book also gives the reader good knowledge about the chaos of war. Even though the British Army is famed as a credible and experienced fighting force, Mr Mervin's account makes clear how, from the moment he arrived in Iraq, day-to-day operations were replete with confusion and mishaps – such as the farcial and incidental way he is eventually assigned to his unit or blundering into a new US artillery range which the Americans had not informed the British about. It gives added credence to the axiom that the best laid plans and battle orders never survive contact with the enemy. What seems to get Mr Mervin and his fellow soldiers through is good training, common sense and a bit of luck. Numerous comparisons are also made between British Army and US military culture; the impression conveyed is the average British squaddie often has and takes more initiative than his often younger and more procedure-bound US counterpart. Significantly, British Army warrant officers and officers seem to give their men a lot of leeway and expect them to exercise their discretion accordingly.

The book also vividly illustrates the gap in values between soldiers like Mr Mervin and society. He makes repeated criticisms of what he sees to be media bias against the military as well as using choice words to denigrate those who demonstrate or argue against the operations in Iraq. He expresses bitterness about how his call up cost him his job, how employers were reluctant to take him on because they feared that he would be called up for duty again and how he feels that the Ministry of Defence has abandoned him. Ironically, factors like the lack of financial and job security have combined to force him to leave the TA, thus further diminishing the pool of

personnel that have combat experience in Iraq. It vividly illustrates how the military requires support from wider society in order to be fully effective.

In his moral certainty, that the war in Iraq was a good war, Mr Mervin is definitely closer to the Bush and Blair positions than Prof Chan. However, Mr Mervin's relatively short stint of about three months (his tour of nine months was prematurely cut short by a broken thumb) of the initial phase leading up to the capture of Baghdad also means that he did not experience the subsequent situation of Iraqis attacking their self-proclaimed liberators, of being worn down and disillusioned by incessant insurgent ambushes against US and UK forces in Iraq or the slow pace of restoring basic public services like electricity, water and health care.

While both books deal with the Iraq war, their positions and perspectives are hugely different. Being a personal account, Mr Mervin's story has a strong air of authenticity. Like other accounts from the lowest ranked, like former US infantryman Colby Buzzell (*My War: Killing Time in Iraq*) and ex-US National Guardsman John Crawford (*The Last True Story I'll Ever Tell: An Accidental Soldier's Account of the War in Iraq*), *Weekend Warrior* provides up-close insights into the mind of the ordinary soldier on the ground – the one who is in the thick of the fighting at the risk to his or her own life and gives a fuller picture to what we know from official sources, mass media and books by commanders and seniors officers. While officially sanctioned publications such as *Shoulder to Shoulder: Commemorating 35 Years of National Service* and Mickey Chiang's *Fighting Fit: The Singapore Armed Forces* are notable for their bottom-up approach, individual SAF personnel and leaders have not produced a comparable body of reflective autobiographical literature.

In conclusion, the autographical nature of *Weekend Warrior* is more endearing, this approach is still largely an anecdotal one. In a praiseworthy effort by a thinking soldier, Mr Mervin share his views on the larger issues like the morality of the war and the effectiveness of the British versus American ways of war. However his mission is to limited to telling us his own very personal story and does not critically engage with different views. This illustrates how *Out of Evil*'s macro treatment is an altogether more systematic and thought-provoking but no less accessible or important contribution to the debates on some of the most significant events of our times.

Mr Toh Ee Loong is currently pursuing his PhD overseas , reading Asian Politics at the School of Oriental and African Studies, University of London, U.K. He obtained a BSc (First Class Honours) in International Relations from the London School of Economics and Political Science in July 2000 and a MA in War Studies from King's College, London in Sept 2001. He served as the Assistant Editor, POINTER for three years, relinquishing the appointment in Feb 2005.

FEATURED AUTHOR

Stephen Chan

Stephen Chan is currently a Professor of International Relations in the University of London, and foundation Dean of Law and Social Sciences at the School of Oriental and African Studies. He is also the General Editor of International Relations for I.B. Tauris. Professor Chan was born in 1949 in New Zealand, and his parents were refugees at that time. He obtained his Master's Degrees from both the University of Auckland and London University's King College, and later received his PhD from the University of Kent. Chan has been blessed with an illustrious academic and political career spanning three decades ever since, previously holding senior positions at the University of Kent and Nottingham Trent University. He has lectured in five continents, and more notably, has been Visiting Fellow at Queen Elizabeth House in Oxford twice.

It is written on Chan's official website that "Professor Chan has always sought a praxis in his life", that is, he has always been keen in translating his ideas into action. Throughout his life, Chan has had the privilege of perspective. As an international civil servant, he has been serving in countries of contrast, from London to Lusaka. He was also seconded to the Commonwealth Observer Group that oversaw the independence of Zimbabwe. As a keen academic, he has been on the executive committee of the David Davies Memorial Institute of International Studies, and as Adviser to the Academy of Finland. Chan's immensely diverse treasure cove of experiences has given his written works depth and scope – they are not limited to merely a continent or an era, but span the major political and military milestones of the world over the last 30 years. In his personal life, Chan is actively involved in the literary and martial arts scene, and has founded the Kwok Meil Wah Foundation in his quest to bring martial arts to the underprivileged areas of Africa.

Chan's latest critically acclaimed masterpiece, *Out of Evil: New International Politics and Old Doctrines of War*, questions the efficacy of the use of the term "Axis of Evil" in modern international politics. He states that it is essentially a conviction of the current American President, and that it is crucial to evaluate the moral and historical validity of the term and warns against the potential political backlash of policy makers today. It is gathered from the book that perhaps the gravest danger is not so much the political and/or military threat that countries like Iraq pose, but rather, that the term "evil" is too liberally used to describe these countries which are in turmoil. Chan concludes that the root cause of the threat should be weeded out and eliminated, rather than going for the blanket solution of waging war against the country "with unprecedented might". In line with the metaphor of a skilled surgeon, the virus should be identified and destroyed using a scalpel and a microscope, not a sledgehammer. The ideas of the book are strengthened by both moral reasoning and historical backing, and warns of a possible retaliation in the form of a large scale war against the US from the countries she is currently in conflict with. Hence, the relevance of *Out of Evil: New International Politics and Old Doctrines of War* is extremely impressive, and it challenges the reader to remove the rose-tinted spectacles and see the possible consequences of the actions of political and military policy makers today.

Theories of International Relations is a compilation of 80 articles written by some of today's most influential international relations scholars, and is divided into four thematic volumes. This intensely provocative publication examines the contemporary relevance of modern international relations and critical geopolitics. Its opening essay is written by both Professor Chan and Cerwyn Moore, and this is in line with *The Zen of International Relations: IR Theory from East to West.* Edited by Chan and Peter Mandaville, the works in this publication question the very fundamentals of international relations and what we know of them. Culture plays a far more crucial role than we think in the shaping of international politics, and the relations of power between countries of contrasting cultures stem from the basic historical differences that make them drastically different in the shaping and understanding of politics. Ironically, however, even with the advent of globalisation over the last two decades, it is shrewdly noted that it is ultimately the embracing of one's unique culture and way of thought that will ensure the long term survival and endurance of a country. Hence, it can be observed that Chan is one who does not accept a given term or ideology at face value, but is instead bold enough to challenge the fundamental assumptions of that ideology.

Given Chan's multi-faceted life experiences in Africa (he has lived in Zambia, and has trained ministries in Zimbabwe, Kenya, Uganda and Ethiopia), it comes as no surprise that he is deeply rooted in the continent and its political and military history. In the powerfully written *Robert Mugabe: A Life of Power and Violence*, Chan traces Mugabe's degeneration from a successful and well-liked nationalist leader to a dominating political tyrant who kept a tight rein over the media and brutally silenced the opposition. It

is important to clarify that the purpose of the book was not to emphasise the failures of Mugabe or portray him as the villain, but rather, serve as a reminder of how extenuating circumstances can bring a purposeful and promising leader to his knees. For instance, Mugabe led a successful resistance against the policy of apartheid in South Africa, but circumstances such as the debacle of the Congo War, increasing internal corruption and the advent of the AIDS crisis had degenerated this potentially great leader into a dominating despot hell-bent on clinging onto his position. The book serves its role as a timely reminder to politicians and strategists to hold true to their beliefs and not conform to conditions that may threaten to sway their political principles.

Chan's prolific knowledge of the African continent becomes ever clearer in *War and Peace in Mozambique*, co-written with Moises Venancio, Chris Alden and Sam Barnes. In the chapter "War and Gropings Towards Peace", Chan's research on the neighbouring countries' policies towards Mozambique is evident, and he states that the front-line states not only intervened openly in Mozambique, but also operated surreptitious units behind Resistencia Nacional Mocambicana (RENAMO) lines. It is clear that Chan's evaluations are backed up by first-hand experiences of the described situation and interviews with the relevant individuals. All in all, Chan and his co-authors have masterfully combined and addressed issues in territories that few others would have dared venturing into: the concepts of insurgency and guerrilla warfare in the Angolan-Mozambican

context; the region's economic struggles made worse by war, mismanagement, and natural phenomena such as drought, and the critical role played by the front-line states. In essence, the apartheid in South Africa was the ultimate enemy, and the regime's quest to destabilize the neighbouring states to strengthen its policies along racist lines had led to a series of political and military conflicts. What we could take away from the lessons in South Africa is the importance of zero-tolerance towards the policy of preferential treatment of certain races in some countries, and to embrace our belief in meritocracy and democracy as the correct ideologies. *War and Peace in Mozambique* is not for the common reader, but rather, its readership may be limited to individuals having in depth knowledge of the history and politics of Africa. However, it richly rewards the keen reader, and Chan's brilliant ability to draw universal political lessons from the vaults of history becomes apparent once again.

Ultimately, Professor Stephen Chan is nothing less than a masterful author, a commanding authority in today's international political arena. Not only is he an expert on African and American affairs, he is also in the perfect position to give commentary as few other authors have been blessed with the privilege of having first-hand experience living and teaching in all the major continents. To quote famous English poet William Blake, Professor Chan has "see(n) the world in grain of sand". His experiences have culminated in his written works, which are thought-provoking, accurate and often provide readers a fresh perspective: from a first person's point of view.

CDF Essay Competition 2005 Winners

First Prize
Globalisation and Transnational Terrorism: Ironies, Interactions and Implications
LTA Wee Wei Sheng, Edward

Second Prize
The Laments of Cassandra: Reflections on Warning Intelligence in the Information Eden
CPT Guo Jing Hua

Third Prize
Modern Peacekeeping Operations and its Implications on the Role of the Militaries in Asia
LTC Ang Kheng Leong, Benedict

Merit Awards

Self Defence in Peril – The Israeli Attack on Osiraq
LTC Lim Teng Chye, Lawrence

Near Space, Near Future
MAJ Jeoh Leo

Social Capital: Cultivating this Vital Element for the 3rd Generation SAF
CPT Fan Sui Siong, Kelvin

"3rd Generation SAF without a 3rd Generation Officership?" A Sociological Analysis of the Implications of Contemporary Socio-political Developments on Officership in the SAF
CPT Lim Yu Sing

Fishing in Troubled Waters: Sino-ASEAN Relations and the South China Sea
CPT Yong Wei Hsiung

Are Force Modernization Dynamics or Regional Norms Responsible for Southeast Asian Security?
CPT(NS) Wong Tze Yung

Transforming an Army: Military Leadership and Military Transformation in the British and Indian Armies
LTA(NS) Toh Boon Ho

Commendation Awards

Science, Technology and War
LTC Gurbachan Singh

The Security of Sea Lanes in Southeast Asia
LTC Ho How Hoang, Joshua

Who Lost the War – The Over Promise of RMA or Poor Strategy?
LTC Ngoh Sien Sen, Charles

The Transformational Leader: Beyond Charismatic Leadership
CPT Lee Yew Chuan, Gerald

Our People: Resource or Capital?
CPT Lim Boon Cheow

Re-examining Military Options for Counter Terrorism
CPT Sim Kai

Is Humanitarian Relief Operation Contrary to Combat Operation? A Reconciliatary Approach
CPT Wee Xun Ming, Elijah

Soldier Empowerment: Human Force Transformation
LTA Phua Chao Rong, Charles

Managing Intellectual Property in Procurement
Mr Kow Keng Wee

PRIZES FOR THE ANNUAL CDF ESSAY COMPETITION

- First prize - $1500 and a plaque
- Second prize - $1000 and a plaque
- Third prize - $500 and a plaque
- Seven Merit awards - $300 and a plaque
- Ten Commendation awards - $300 and a certificate

CDF Essay Competition – 2006

POINTER is pleased to announce the
20th Annual Chief of Defence Force Essay Competition.

The CDF Essay Competition aims to encourage SAF Officers to conduct research on professional and military-related issues relevant to the SAF. You are invited to share your knowledge, ideas and reflections on war fighting/force transformation, leadership/organisational development, or conflict & security studies. All competition entries must be submitted in soft copy and be accompanied by a soft copy form. The Entry form can be downloaded at the revamped *POINTER* website @ http://www.mindef.gov.sg/safti/pointer.

All Regular/Full-time National Service/National Service Officers, Officer Cadets, Warrant Officers, Defence Executive Officers and Defence, Science & Technology Agency personnel are welcome to participate.

Submit your entry early. The CDF Essay Competition 2006 is closing on 31 Dec 06.

CDF Essay Competition 2006

Essay Title:_____ (Word Count: _____)

Rank/Name:_____ NRIC:_____

Gender: <u>M / F</u>*   Unit:_____

Service: AIRFORCE / ARMY / NAVY / JOINT / DSTA / OTHER*

Service Status: REGULAR / NSF / NSMAN / DXO / DSTA*

Home Address:_____

_____

Office Tel No:_____

Mobile Tel No:_____
(So we can contact you if you are posted out)

E-mail:_____

Educational Profile (HSP)

(Qualification, Institution and Year of Award):_____
All competition entries which are not accompanied by this form will be rejected. All fields must be completed. Non applicable fields must be marked with "NIL" or "N/A". Thank You for your co-operation.

Please delete accordingly.

POINTER: Journal of the Singapore Armed Forces

SUBSCRIPTION ORDER*
3 years 12 issues $12.00 ($1.00 per issue)

NRIC No/Rank/Name _____

Unit _____

Home Address _____

_____ Postal Code _____

Office Address _____

_____ Postal Code _____

Telephone (Home) _____ (Office) _____

Payment enclosed Cheque No. and Bank _____

A. PAYMENT BY CHEQUE
Crossed cheque to be made out to *'Permanent Secretary, Ministry of Defence'*. Send this form and cheque to:

> MINDEF Cashier,
> D'eXecutive Services
> 5, Depot Road #15-01,
> Defence Technology Tower B
> SINGAPORE 109681

B. PAYMENT BY PAY DEDUCTION (ACTIVE SERVICEMEN ONLY):
Send back this form by fax to 6799-7758 or by post to:

> EDITOR *POINTER*
> SAFTI MI, Military History Branch
> 500 UPPER JURONG ROAD
> SINGAPORE 638364

I authorise the deduction of $12.00 from my pay for the purpose of subscribing to *POINTER* for 12 issues.

_____
                                                          Signature / Date

* NSmen can opt to subscribe to *POINTER*. In-service military Officer, Warrant Officers and DXOs (Grade 8 and above) are automatically subscribers of *POINTER* upon enlistment.

Please inform your AO or Chief Clerk within 14 days of any change in address for our database to be updated.